LockView® NTC/VTC 4.3.3

LOCKVIEW NTC/VTC INSTRUCTION MANUAL

Instruction Manual

Snap-on®

TABLE OF CONTENTS

LockView NTC/VTC Instruction Manual

Introduction **4**
Operation **5**
LockView Login 5
Screen Information 6
Operator Editor **7**
Lock/User Editor
User Editor 9
Lock Editor (NTC) 15
Lock Editor (VTC) 20
Access Rights 25
Group Editor 26
Read/Write Lock
Connection 29
Read Slots 31
Audit Trail 33
Lock Settings 36
Notifier (NTC) **38**
Technical Setup 38
eReports 40
Notifier (VTC) **43**
Add Responder 44
Edit Responder 45
Delete Responder 45
Global Lock Settings 46
Technical Setup 47
eReports 49
Compliance Dashboard 51
Programming Example **54**
Settings **64**
Create ODBC Connection for an Existing Access Database **65**
Create ODBC Connection for New Access Database **67**

NOTE:

The Table of Contents contains live links. Click on any section, and the corresponding page will load.

TABLE OF CONTENTS continued

Other manuals available as separate pdfs:

- ***Database & Network Configuration & Install Manual***
- ***Manual Programming of the Snap-on Level 5 Gen3 Lock***

IMPORTANT NOTE:

Certain features noted in this manual only apply to Snap-on NTC or VTC systems. These sections are clearly noted at the beginning of the section. Pictures of NTC and VTC are shown below as a reference.

VTC

NTC

INTRODUCTION

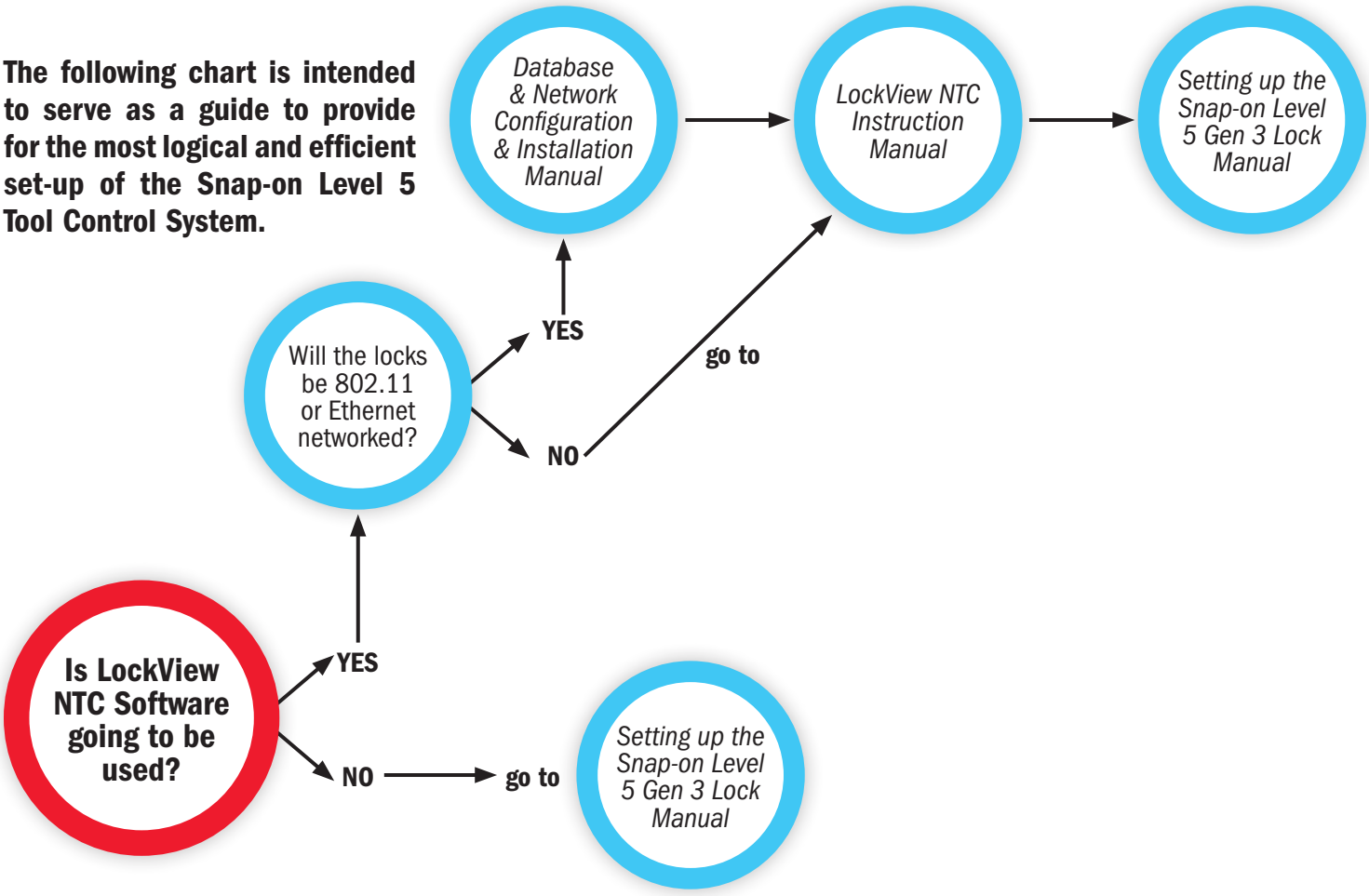
An authorized Operator of LockView® can create a database of users and locks on a local or networked computer. Each user in this computer's database is assigned to a slot in each lock to which they have access. A lock's internal memory is divided into 999 slots that store user information thereby giving each lock a maximum of 999 users. That is, 999 individuals are capable of opening the toolbox.

The computer on which LockView® is loaded has the ability to connect to locks directly, through a USB dongle or through a computer network, using Ethernet or 802.11g Wi-Fi, and update the lock's memory to correspond with its own database. It is able to gather and manipulate a lock's audit trail, or past operation log. Audit trail information contains the lock's name, the name of the user attempting to gain access, the credential used, if access was granted or denied, and the date and time of each interaction.

LockView NTC 4 works with LockServ to communicate with locks. LockServ has the ability to communicate with multiple locks simultaneously over a computer network, thereby eliminating the need for the Operator to visit each lock to update its database, or download audit trails.

Alternately, LockServ can communicate with locks using a USB dongle if network hardware is not available.

The following chart is intended to serve as a guide to provide for the most logical and efficient set-up of the Snap-on Level 5 Tool Control System.


Database & Network Configuration & Installation Manual
LockView NTC Instruction Manual
Setting up the Snap-on Level 5 Gen 3 Lock Manual
Will the locks be 802.11 or Ethernet networked?
YES
NO
go to
Is LockView NTC Software going to be used?
YES
NO
go to
Setting up the Snap-on Level 5 Gen 3 Lock Manual

OPERATION

Double click the LockView® icon on the desktop to open and run the LockView program.

NOTE: ***If the LockView® ODBC entry was not created properly, it will need to be created manually. Refer to*** **DATABASE FILE LOCATION** on page 67.

LOCKVIEW® LOGIN

Double click the **LockView** icon on the desktop. The below window will appear:

For first time Login, enter "**admin**" under both Operator Name and Password. Click **OK**. **NOTE**: Password is case sensitive.

➔ After an Operator has been added to LockView, use of personalized **Operator Name** and **Password** should be used for Login.

See *Database & Network Configuration & Install Manual* for more information.

OPERATION continued

NOTE: *There is NO security while logged in under "admin." The "admin" user should be deleted after a new Operator Name and Password have been completed to ensure database security.*

SCREEN INFORMATION

FILE drop down menu – Used to EXIT program.
VIEW drop down menu – Used to display or eliminate the shortcut and/or status bars on the program screen; display or eliminate the background image; select another background image from a saved file; or return program to default settings.
WINDOW drop down menu – An alternate way to access the following programming menus:

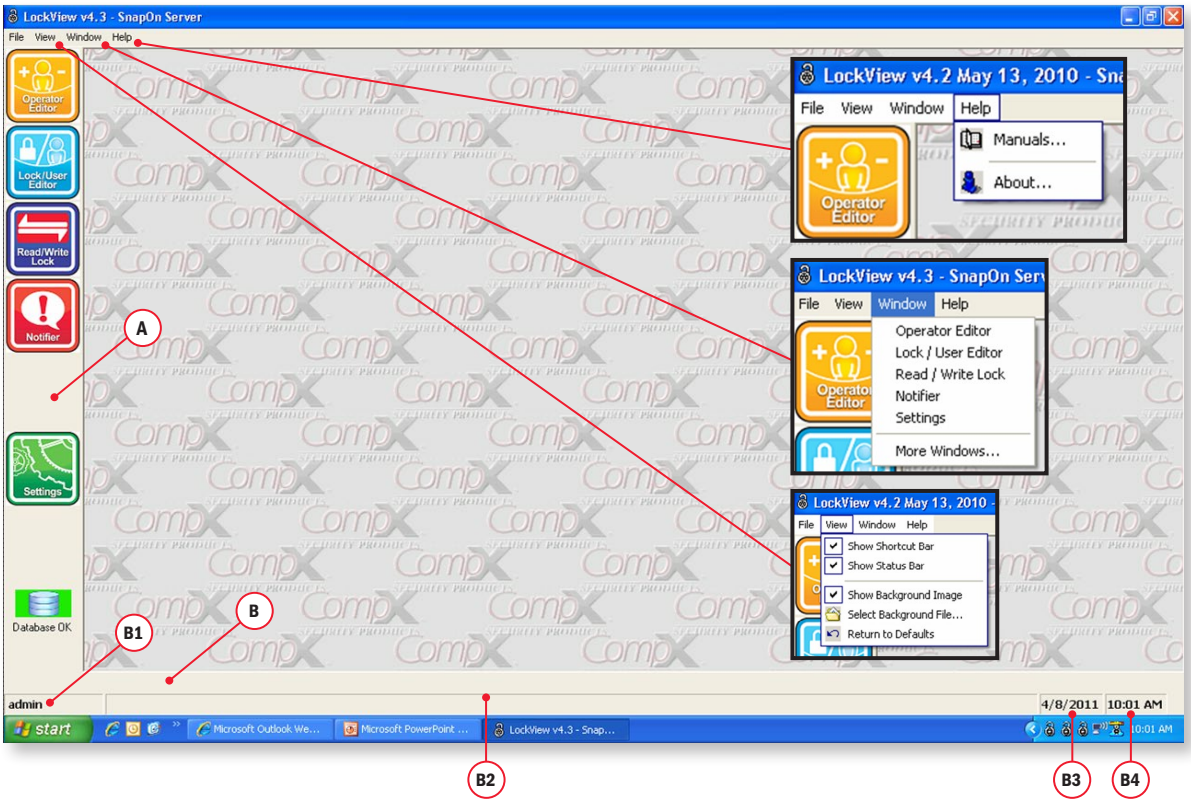
- Operator Editor
- Lock/User Editor
- Read/Write Lock
- Notifier
- Settings
- More Windows

HELP drop down menu – pdf of LockView User Manual.

A **SHORTCUT BAR -** Quick start buttons for the **Operator Editor, Lock/User Editor, Read/Write Lock,** and **LockView® Options** menus. The shortcut bar can be displayed or hidden, refer to the **VIEW** drop down menu.

B **STATUS BAR -** Displays the following LockView program status information:
B1 – Name of Operator that is currently logged into software.
B2 – "Connected to" lock status. Displays the lock to which LockView is currently connected as well as the connection status: **In Sync** or **Needs Update.**
B3 – Current local computer date.
B4 – Current local computer time.

NOTE: The status bar can be displayed or hidden, refer to the View drop down menu.



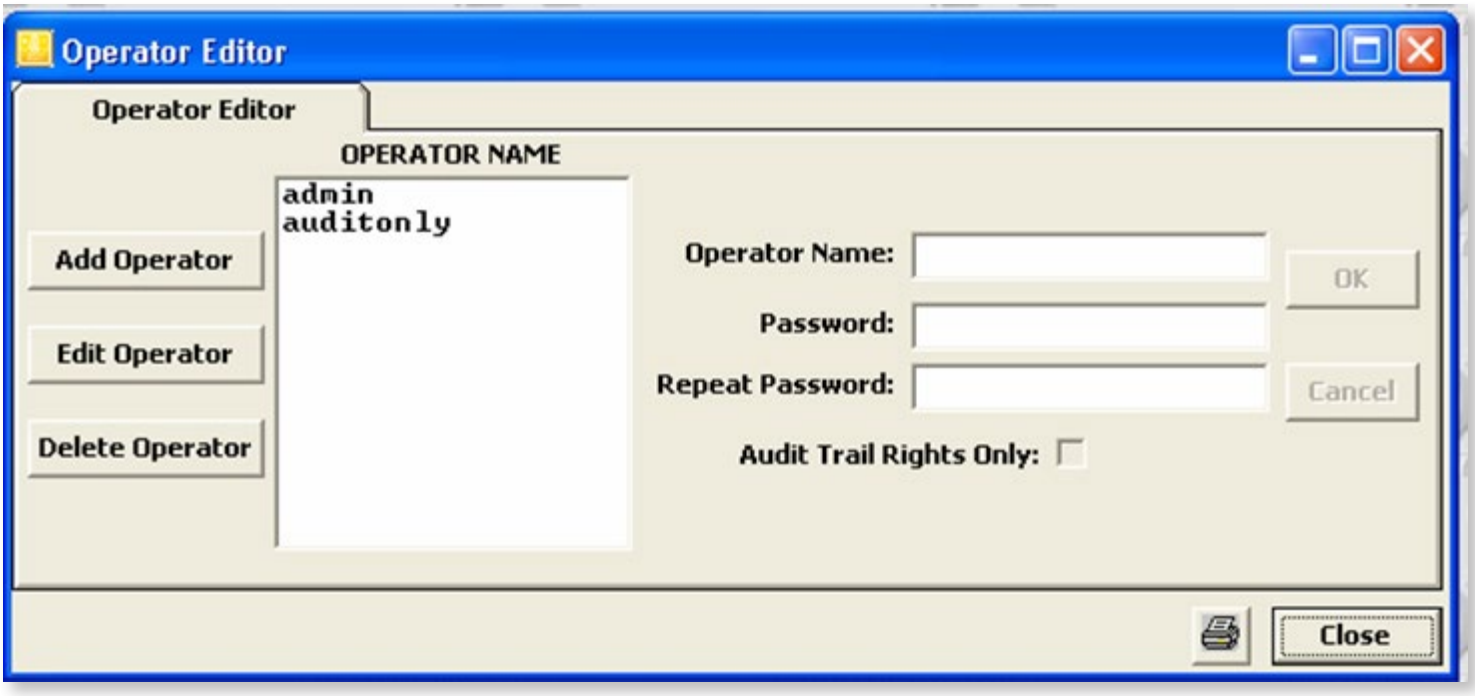
OPERATOR EDITOR

An Operator is someone who is responsible for building and maintaining a database of users and locks. An Operator does NOT have to be a user of locks. The **Operator Editor** window allows the Operator to create new Operators. New Operators can be given full access or Audit Trail Rights Only.

➔ The deletion of the logged-in Operator is prohibited.

NOTE: *After the first new Operator is added, exit LockView and login as the new Operator. Delete the "admin" Operator.*

NOTE: *First Operator added to LockView® should be given full access rights.*



TO ADD A NEW OPERATOR

1. Select the **Operator Editor**.
2. Select **Add Operator** to create a new Operator.
3. Enter the new Operator Name and Password.
   ➔ If **Audit Trail Rights Only** is chosen, the Operator will only be able to retrieve and view audit trails.

NOTE: *Passwords are case sensitive and must be a minimum of 4 characters.*

4. Select **OK** when done.
5. Select **Close** to close the Operator Editor tab.

TO EDIT AN OPERATOR

1. Select **Operator Editor**.
2. Select **Operator Name** and then select **Edit Operator** to edit an Operator's information.
3. Select **OK** when done.
4. Select **Close** to close the **Operator Editor** tab.

OPERATOR EDITOR continued

TO DELETE AN OPERATOR

1. Select the **Operator Editor**.
2. Select **Operator Name** and then select **Delete Operator** to delete an existing Operator.

   NOTE: *Deletion of the currently logged in Operator is prohibited.*

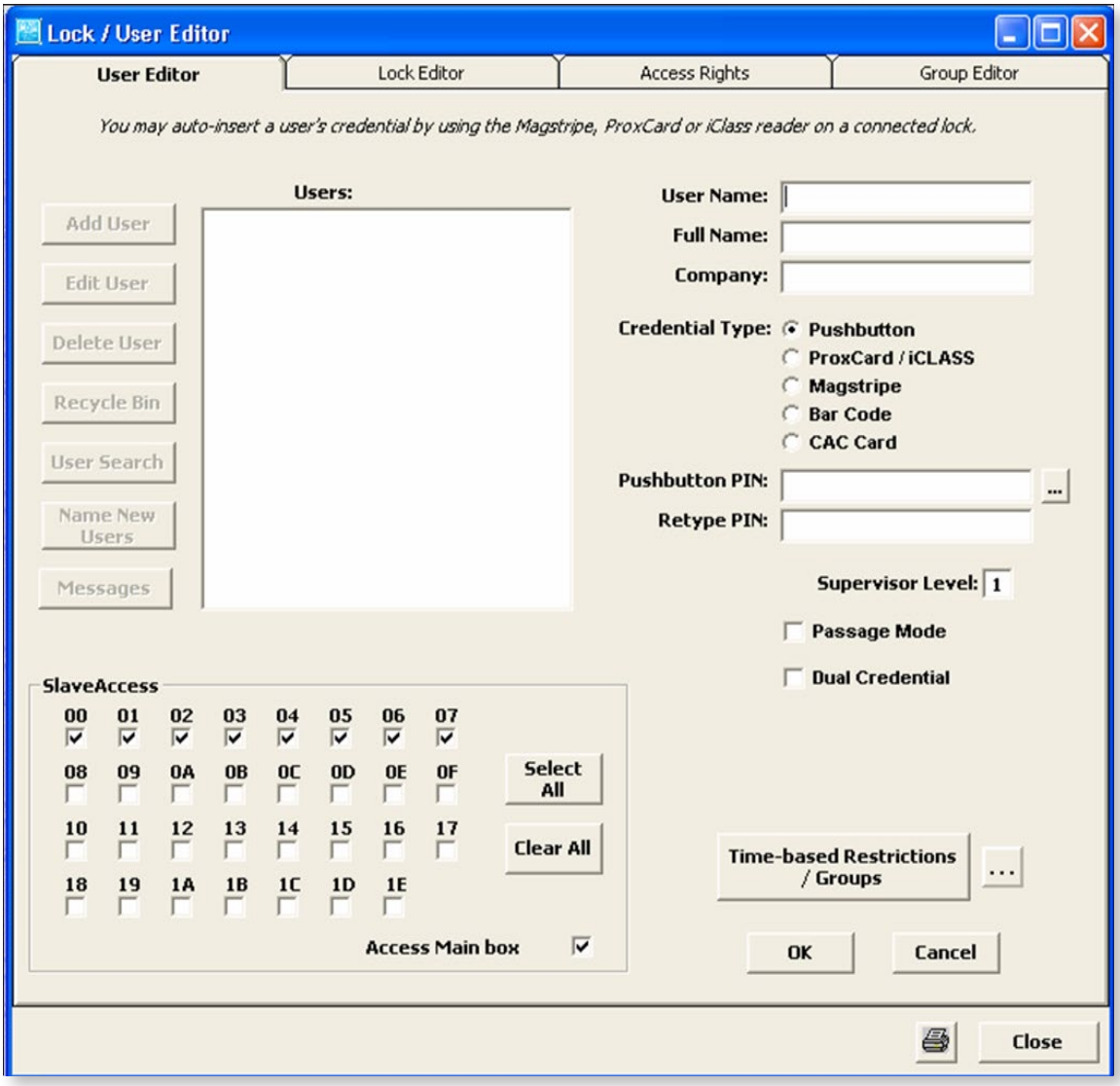
3. Select **Close** to close the **Operator Editor** tab.

LOCK / USER EDITOR

The **Lock/User Editor** window allows the Operator to modify the user and lock databases.

USER EDITOR

The **User Editor** tab is used to add, edit or delete users from the computer database.



TO ADD A NEW USER

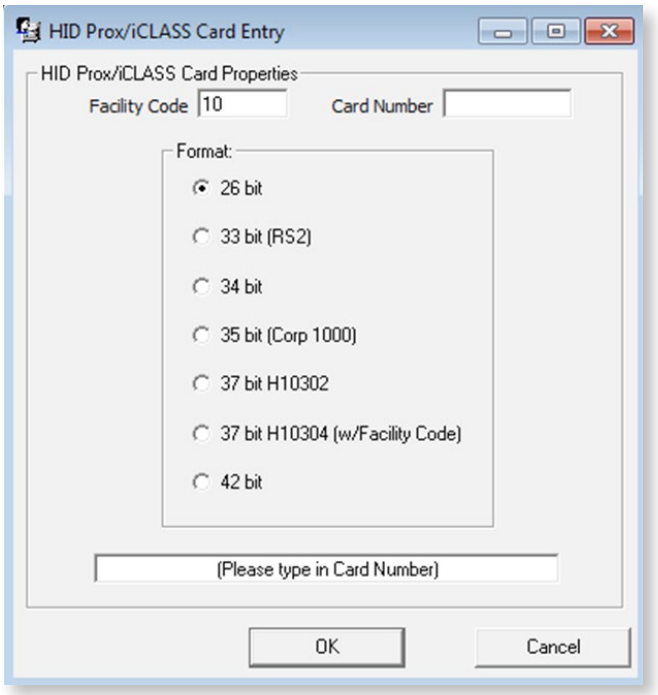
1. Select the **Lock/User Editor**.
2. Select **Add User** to create a new user in the database.
3. Enter the new user's information.
   User Name must be a minimum of 4 and a maximum of 14 characters.
   The user's **Full Name** and **Company** are optional. **User Name** is required and will appear in other places and reports in LockView.
4. Enter the new user's credential information.
   - ➔ If the user is to have a PIN (pushbutton) credential, press the more info button [...] next to the pushbutton PIN field to generate a random PIN.
   - ➔ If an unit is connected at the time, and is equipped with a magstripe card reader, HID Prox reader, HID iCLASS reader, or a bar code reader, select the proper **Credential Type** and present the card to enroll the information automatically into the database. (HID Prox and iCLASS are both read under **ProxCard**)

LOCK / USER EDITOR continued

➔ To manually input an HID credential (Prox or iCLASS), select **ProxCard** and click the more info button [...]. The HID **Facility Code, Card Number,** and **bit Format** are needed in order to enroll a proximity card manually. This information can be obtained from the purchaser of the HID cards.

NOTE: *Use of the more info button [...] is optional and not required to generate a PIN or HID prox credential.*

➔ Choose the HID Format (26, 33(RS2), 34, 35, 37 bit, 37 bit with facility code, or 42 bit)

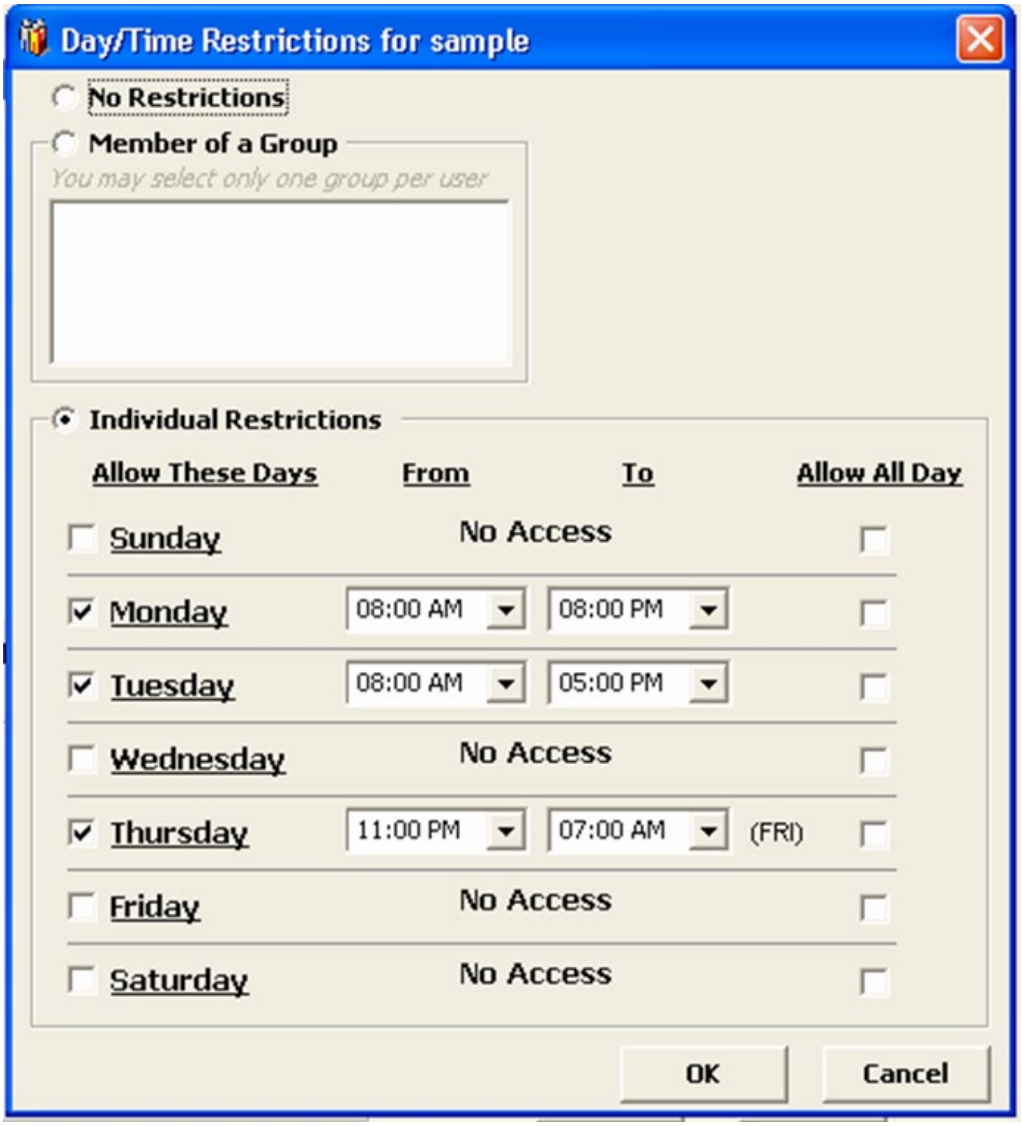


➔ Enter the **Facility Code** (if that format has a facility code)
➔ Enter the **Card Number**
➔ The hexadecimal number corresponding to that **Format**, **Facility Code**, and **Card Number** will appear in the box. Clicking **OK** will automatically transfer that number into the **User Editor**.
➔ A user can have one "primary" credential (PIN, prox card, mag stripe or barcode) as well as a secondary PIN credential if they have dual credential rights.

NOTE: *Two users cannot have the same PIN or card credential. This includes users in the Recycle Bin. If a credential is "recycled," the user who was previously using the credential must be completely removed from the database. (Including from the Recycle Bin.)*

5. If the new user has supervisor rights, choose the **Supervisor Level** in the corresponding box. Supervisor levels 1-9 may be chosen; where 1 is the lowest level and 9 is the highest level. Supervisor rights are especially useful for programming locks without the LockView software.
6. If the new user has **Passage Mode** rights, check the **Passage Mode** box next to the credential information being supplied. **Passage Mode** allows the user to change the lock's state (lock/unlock) by pressing "Enter" (at the lock) after the PIN or card has been accepted and the unit is unlocked. **NOTE**: when in passage mode, the lock open time is disabled.
7. If the new user has **Dual Credential** rights, check **Dual Credential** next to the credential information being supplied and enter the dual credential PIN
   ➔ Dual credential users are users that are required to present two credentials in order to gain access.
   ➔ Dual credential users must use a PIN after the primary credential.
   ➔ If the user has a PIN/PIN dual credential, the PIN numbers must be different. (**NOTE**: Primary and secondary PINs are NOT interchangeable.)
8. If the new user will have day and time access restrictions or be a member of a group, select **Time-Based Restrictions/Groups**.
9. If the new user will be a group member, check the button adjacent to member of a group, then click the group name. For more information on groups, go to page 26.

LOCK / USER EDITOR continued

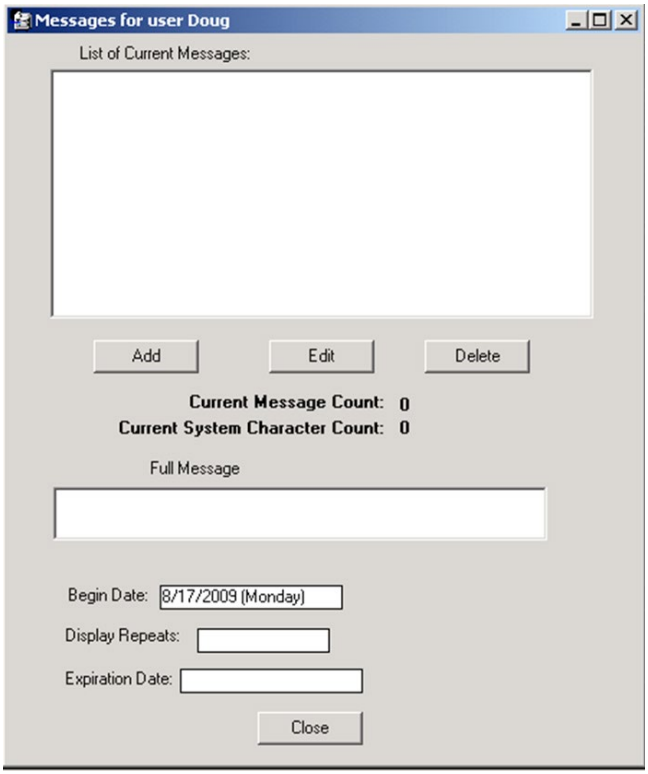


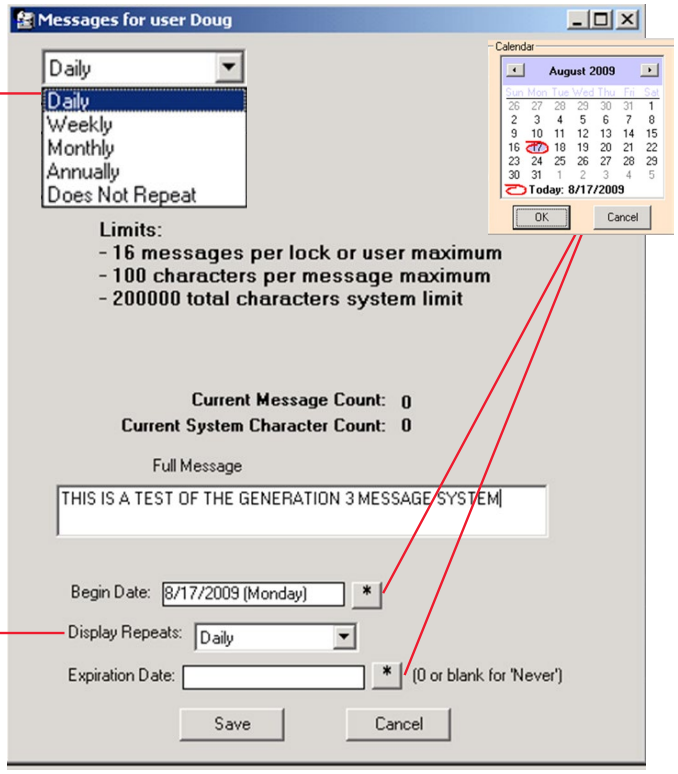
10. Fill in the time slots the user is allowed access, or check **No Restrictions** if the user has 24 hour access. When filling in time slots, LockView will automatically wrap a day. (Example: 11 p.m. Monday - 7 a.m. Tuesday.)
11. APPLIES TO NTC SYSTEMS ONLY: If the user is to have access to slave locks, select the slave(s) in the bottom left section of the **User Editor** under **SlaveAccess**. The slave ID is made up of two digits located on the slave modules. The first digit corresponds to the position of DIP switch 7 (up=1 down=0). The second digit corresponds to the position of the HEX switch. For example, slave ID# 1C would have DIP switch 7 in the up position and the hex switch pointing to C.

    NOTE: *If the user is to have slave access only, deselect "Access Main box." This will give the user access to the slaves only, the main tool box will not open.*

12. Select **OK** when done.

LOCK / USER EDITOR continued

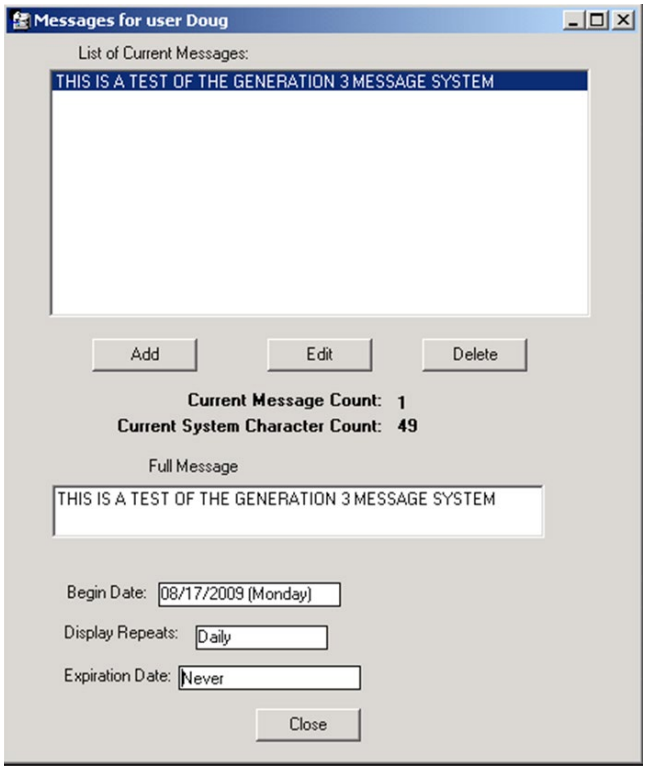




USER MESSAGES—APPLIES TO NTC SYSTEMS ONLY

When a credential is presented to a lock, it is possible for a user to see up to 16 different messages on the access panel display. To add messages in **User Editor**, select the desired user, and click **Messages**. To add a message:

1. Click **Add.**
2. Type the message. **NOTE**: Maximum of 100 characters per message.
3. Choose the **Begin Date** entry box by clicking "*" which will open a calendar. This will be the date on which the message will begin.
4. Choose how often the message will repeat in the **Display Repeats** pull down. **Daily** (every day), **Weekly** (same day of the week), **Monthly** (same day of the month), **Annually** (once a year, that exact date) **Does Not Repeat** (message will appear one calendar day only).
5. Choose the **Expiration Date** entry box. Clicking "*" will open a calendar. This will be the date on which the message will expire.
6. Click **Save** when done.
7. Note that there is a maximum of 16 messages per user.
8. Messages can be edited or deleted by highlighting the message from the **List of Current Messages** and choosing **Edit** or **Delete**.
9. Click **Close** when complete.



LOCK / USER EDITOR continued

TO EDIT A USER

1. Select **Lock/User Editor**. Select **User Editor**.
2. Highlight **User Name** and select **Edit User**.
3. Select **OK** when done. Any changes made to a user must be uploaded to the locks to which the user has access. (See Read/Write Lock.)
4. Select **Close** when done.

TO DELETE A USER

1. Select **Lock/User Editor**. Select **User Editor**.

NOTE: *Before deleting a user, it is recommended the user's access rights be removed from all locks. For more information on access rights, go to page 25. This ensures the user is deleted and will not be accidentally reinstated into the computer database.*

2. Highlight **User Name** and select **Delete User**.
3. Select **Close** when done**.**

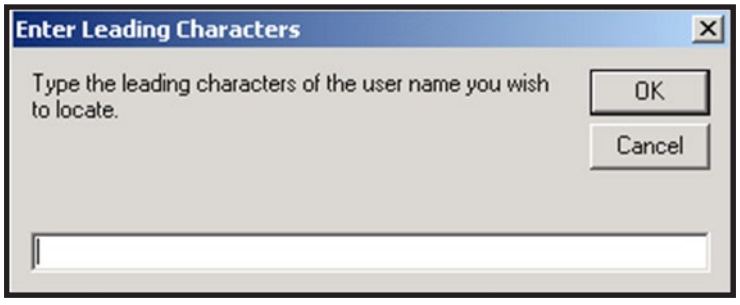
RECYCLE BIN

When a user is deleted from the LockView database, the user is moved into the **Recycle Bin**. Once in the **Recycle Bin**, the user can either be restored to the database or completely deleted from the database.

NOTE (VERY IMPORTANT): *Two users cannot have the same PIN or card credential. This includes users in the recycle bin. If a credential is to be passed to a different user, the person who previously had the credential must be removed from the **Recycle Bin**.*

TO FIND A USER

If a user cannot be found in the **User Editor**, click **User Search.** Enter the first few characters of the user's name and click **OK**.



LOCK / USER EDITOR continued

TO NAME A NEW USER

Manually programmed users entered at the lock will appear as $xxxxxxx. Click **Name New Users** and a window will be opened that will prompt the naming of these users.

Enter the desired **New User Name** and click **Save**.

LOCK / USER EDITOR continued

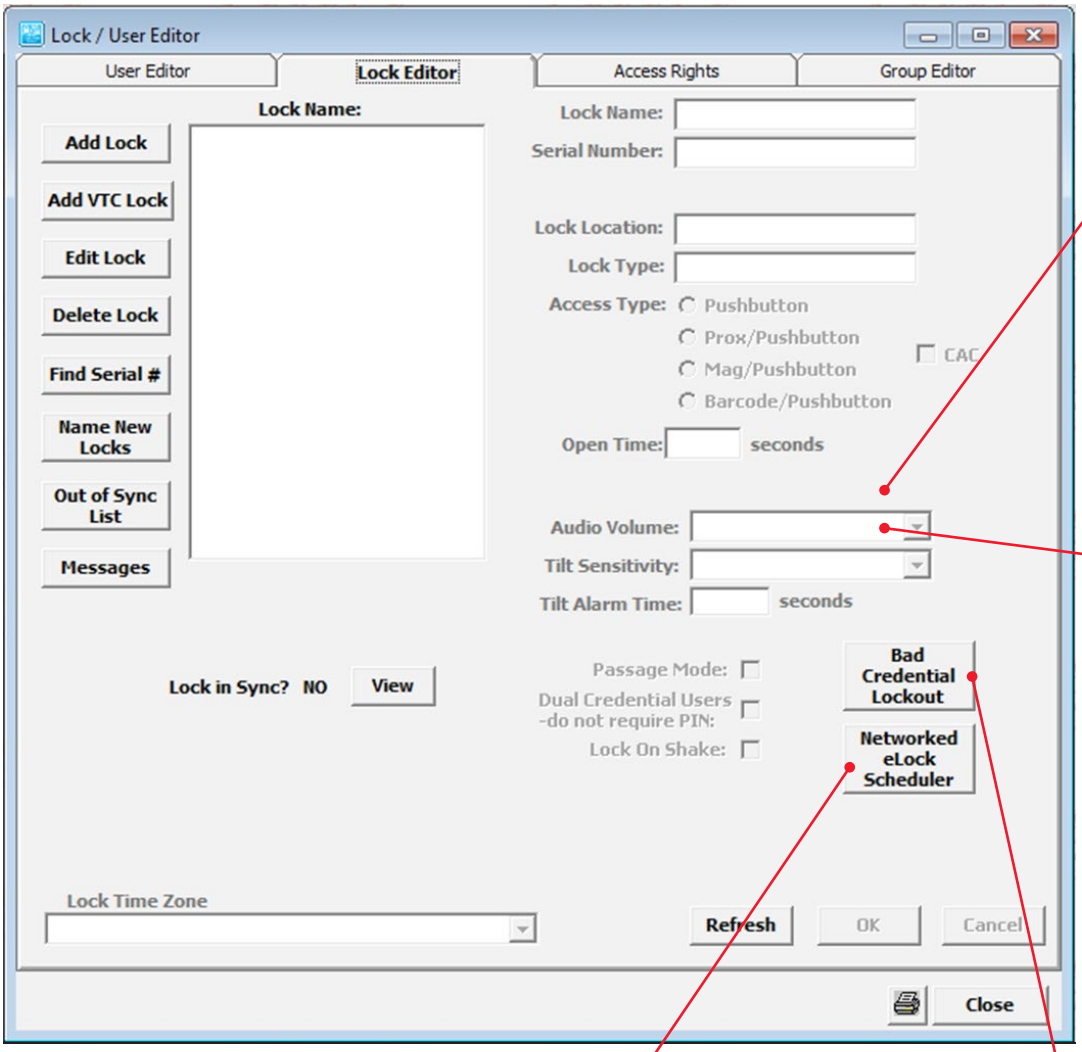
Note: The Lock Editor shown here applies ONLY to NTC systems. See pages 20-24 for VTC systems.

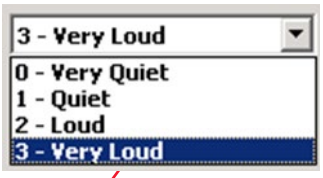
LOCK EDITOR

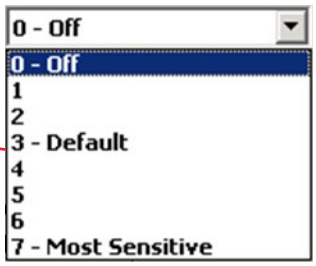
The **Lock Editor** tab is used to add, edit, or delete locks from the database.

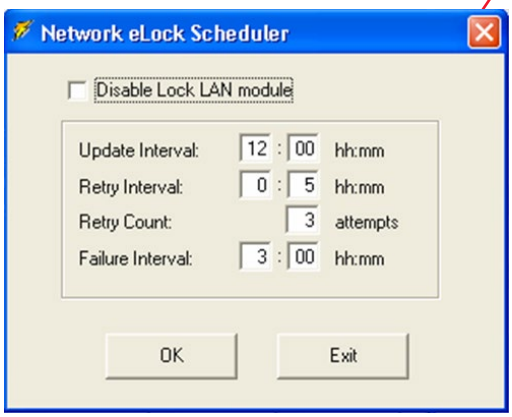
TO ADD A NEW LOCK

1. Select **Lock/User Editor**. Select **Lock Editor**.
2. Select **Add Lock** to create a new lock in the database.









LOCK / USER EDITOR continued

Note: The Lock Editor shown here applies ONLY to NTC systems. See pages 20-24 for VTC systems.

3. Enter a name for the new lock being created. **Lock Name** must be between 4 and 14 characters in length including spaces.
4. Enter the **Lock Serial** and **Setup Code** numbers.
   ➔ **The lock's serial and setup code numbers are on a sticker included with the lock.**
5. Choose the **Prox/Push, Mag/Push, Barcode/Push button** (under access type) if the lock being entered is provided with one of these card readers. **NOTE**: It is not possible to edit a lock's access type. If the lock's access type needs to be changed, the lock must be ***deleted*** and ***recreated*** with the appropriate card reader selected. Prox/Push corresponds to HID Prox and HID iCLASS.
6. If the tool box is provided with the TCMAX system and a CAC card reader, which will be used for tool box access, click CAC.
7. Enter the number of seconds **Open Time (sec)** to program how long the lock will remain open before automatically re-locking.
8. The **Audio Volume** drop down selects how loud the lock will beep upon pressing buttons on the access panel. The available choices are **0-9**; **0** equals OFF and **9** equals loudest.
9. Under "**Tilt Sensitivity**" choose the sensitivity of the tilt alarm. The available choices are **0-7**; **0** equals off and **7** equals the most sensitive. **NOTE**: to enable the tilt alarm, press and hold "Lock" on the keypad. Unit must be locked.
10. The **Tilt Alarm Time** drop down selects the amount of time the tilt alarm will sound (after it is triggered).
11. Click the **Bad Credential Lockout** button to open the bad credential lockout sub menu. The **Bad Credential Lockout** default is **Never Lockout**.
    There are three adjustments:
    a) **After** __ number of **bad attempts**
    b) **In** __ number of **minutes**
    c) **Lockout for** __ number of **minutes**
    For example, after 5 bad attempts in 5 minutes, lockout for 5 minutes.
12. If the lock is provided with an Ethernet or 802.11 module, choose how often the lock will check for updates to the database in the Networked eLock schedule sub menu. Click the "Networked eLock scheduler" button to open. **NOTE**: If the lock does not have a LAN module, choose **Disable Lock LAN Module.**
    a. **Update Interval**- How often the lock will turn on the LAN module and check the network database for updates (enter in HH:MM format)
    b. **Retry Interval**- If the networked lock was unable to connect to the database through the network, enter the amount of time before it retries. (enter in HH:MM format)
    c. **Retry Count**- If the networked lock fails to connect to the database upon retry, the lock will continue to retry the number of times in the "retry count"
    d. **Failure Interval**: If every attempt to connect to the database under the **Retry Count** is unsuccessful, **Failure Interval** is the amount of time the lock will wait before starting the **Retry Interval** again. (Enter in HH:MM format.)

    NOTE*: Each time the lock turns on the LAN module to check the database for updates, a significant amount of energy is drained from the battery.*

13. **Passage Mode** will allow any user to place a lock into **Passage Mode. Passage Mode** will keep the lock in the unlocked state indefinitely. **NOTE**: After a valid credential has been presented and the unit has unlocked, press and hold "Enter" on the access panel keypad to activate **Passage Mode**.
14. If it is desired for dual credential users not to be required to enter both credentials on this particular lock, **Dual Credential Users do not Require PIN**.
15. **Lock On Shake** will allow an open lock to automatically relock upon movement of the unit. The sensitivity of this feature will be identical to the sensitivity of the alarm **Tilt Sensitivity**
16. **Drawer Alarm** will cause the alarm to sound if:
    a) a drawer remains in the open position on an unlocked unit followed by a "Lock" operation (a drawer was left open) or
    b) a drawer is opened on a locked tool box (someone broke in)
    NOTE: optional hardware is required for this feature.
17. Choose the time zone in which the lock is installed under the Lock Time Zone pull down menu. This is helpful if the server and the lock are in different time zones.

LOCK / USER EDITOR continued

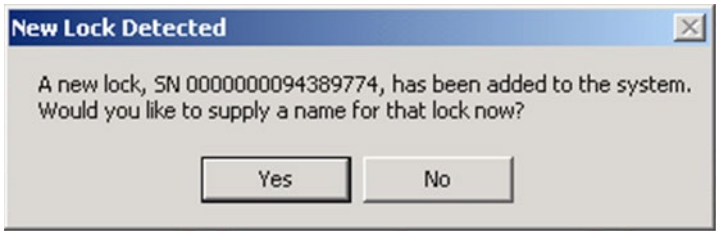
Note: The Lock Editor shown here applies ONLY to NTC systems. See pages 20-24 for VTC systems.

18. Select **OK** when done.

NOTE: *The lock's internal memory must match the database for every setting noted above. The status of the lock setting VS database setting is shown adjacent to* ***LOCK IN SYNC? YES/NO****. If the lock and the database are NOT in sync, the* ***VIEW LOCK SETTINGS*** *button will appear. This button will open the* ***Lock Settings*** *tab in* ***Read/Write Lock****.*

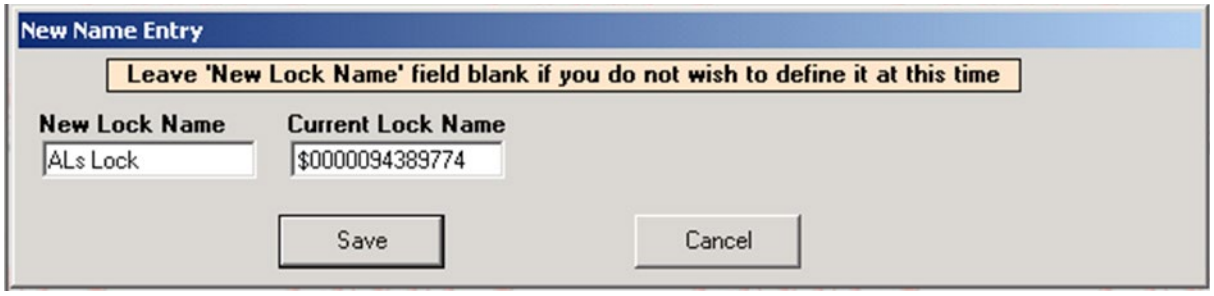
Alternately, the lock can be automatically enrolled into the database.

1. Press and hold "Clear" on the access panel keypad. "SETUP CODE" will appear.
2. Enter the setup code that was provided on the sticker set with the lock into the keypad.
3. Choose "1-UNLOCK" when prompted.
4. "SETUP READY" will appear.
5. Connect the USB dongle to the computer and route the 6 wire RJ11 cable from the dongle to the lock. If a network module is being used and it is setup, press the "Up" button on the keypad to initiate a manual update.


New Lock Detected
A new lock, SN 0000000094389774, has been added to the system.
Would you like to supply a name for that lock now?
Yes
No

6. Within a few seconds, the following window will appear in LockView. SNXXXX is the serial number of the lock being added.

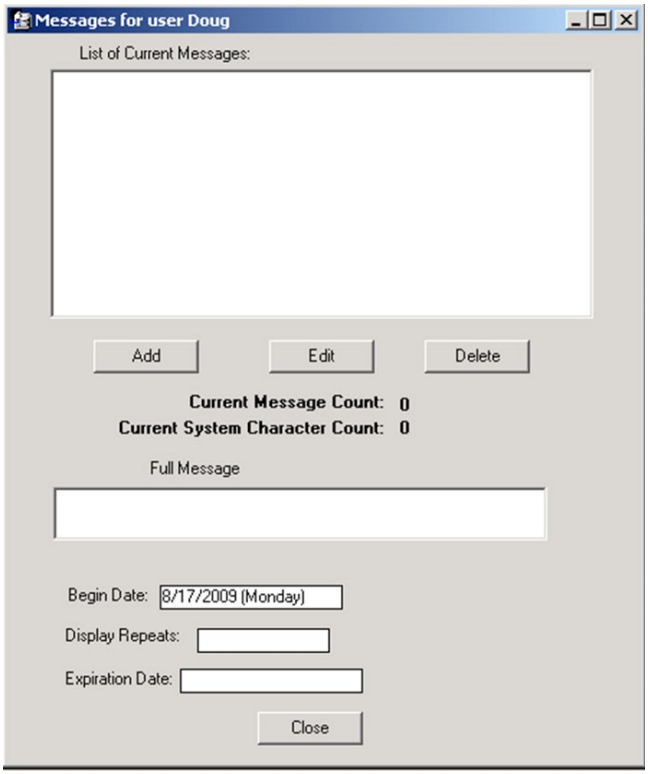
7. Click **Yes.**

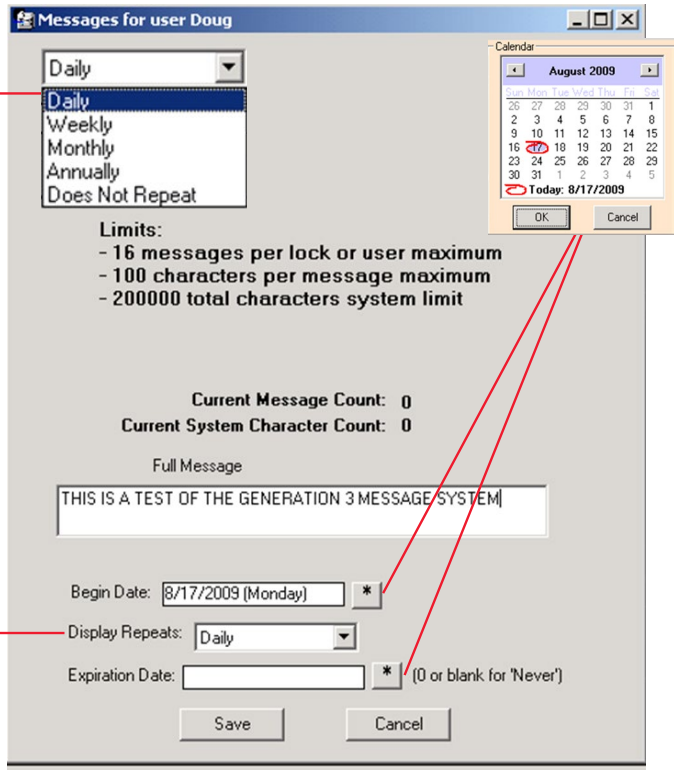


8. Enter the **New Lock Name**. The lock and all of the settings will be loaded into the database.

LOCK / USER EDITOR continued

Note: The Lock Editor shown here applies ONLY to NTC systems. See pages 20-24 for VTC systems.

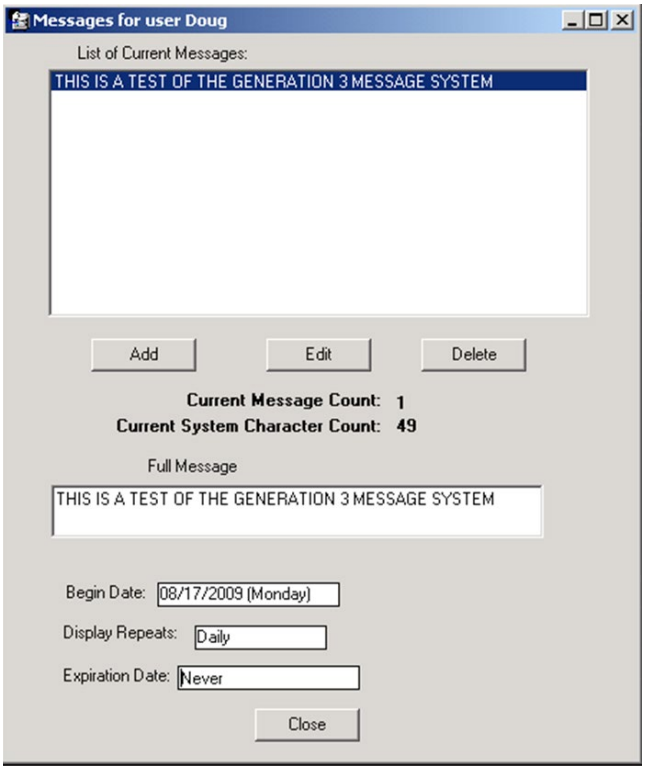




LOCK MESSAGES

It is possible for every user to see up to 16 different messages on the access panel display. To add messages in **Lock Editor**, select the desired lock and click **Messages. NOTE**: Lock messages will appear for every user that has access to the lock. Lock messages are independent from user messages. To add a message:

1. Click **Add.**
2. Type the message. **NOTE**: Maximum of 100 characters per message.
3. Choose the **Begin Date** entry box by clicking "*" which will open a calendar. This will be the date on which the message will begin.
4. Choose how often the message will repeat in the **Display Repeats** pull down. **Daily** (every day), **Weekly** (same day of the week), **Monthly** (same day of the month), **Annually** (once a year, exact date) **Does Not Repeat** (will appear one calendar day only)
5. Choose the **Expiration Date** entry box. Clicking "*" will open a calendar. This will be the date on which the message will expire.
6. Click **Save** when done.
7. **NOTE**: there is a maximum of 16 messages per lock.
8. Messages can be edited or deleted by highlighting the message from the **List of Current Messages** and choosing **Edit** or **Delete.**
9. **Close** when complete.



LOCK / USER EDITOR continued

Note: The Lock Editor shown here applies ONLY to NTC systems. See pages 20-24 for VTC systems.

TO EDIT AN EXISTING LOCK

1. Select **Lock/User Editor**. Select **Lock Editor**.
2. Highlight **Lock Name** and select **Edit Lock**. **NOTE**: lock **Access Type** and dual credential status cannot be edited.
3. Select **OK** when done.

NOTE: *The lock's internal memory must match the database for: Access Type, Lock Type, Open Time, Dual Credential Users do not require PIN, Bad Credential Lockout. To compare the lock settings information and database information, go to the Lock Settings tab under Read/Write Lock and update as necessary.*

4. Select **Close**.

TO DELETE A LOCK

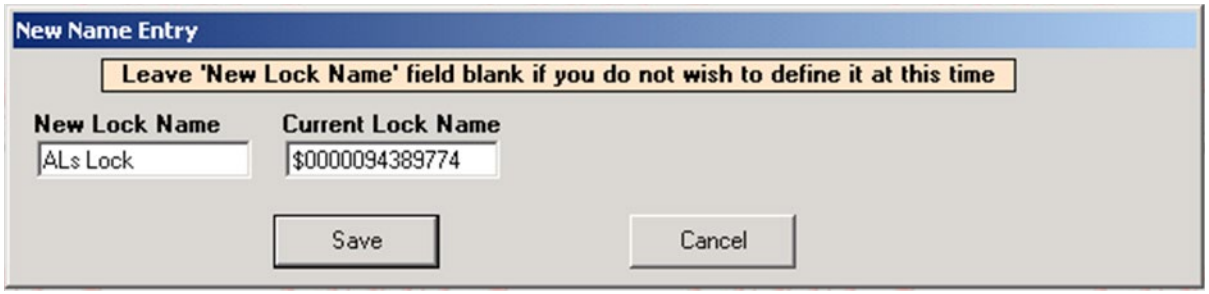
1. Select **Lock/User Editor**. Select **Lock Editor**.

NOTE: *Before deleting a lock, it is recommended to remove all access rights to the lock from all users. This ensures the lock is deleted and will not be accidentally reinstated.*

2. Highlight Lock Name and select **Delete Lock**.
3. Select **Close** to close **Lock Editor**.

TO NAME A NEW LOCK

If a lock was automatically entered into the database and has not been given a proper name; the lock name will appear as $xxxxxxx in the list of locks in the **Lock Editor**, "xxxxxxx" represents the serial number of the lock. To give the locks a proper name, click **Name New Locks.**



OUT OF SYNC LIST

Clicking the **Out of Sync** button will open a window that shows the list of locks that are not "in sync" with the database (lock settings or current users)

LOCK / USER EDITOR continued

Note: The Lock Editor shown here applies ONLY to VTC systems. See pages 15-19 for NTC systems.

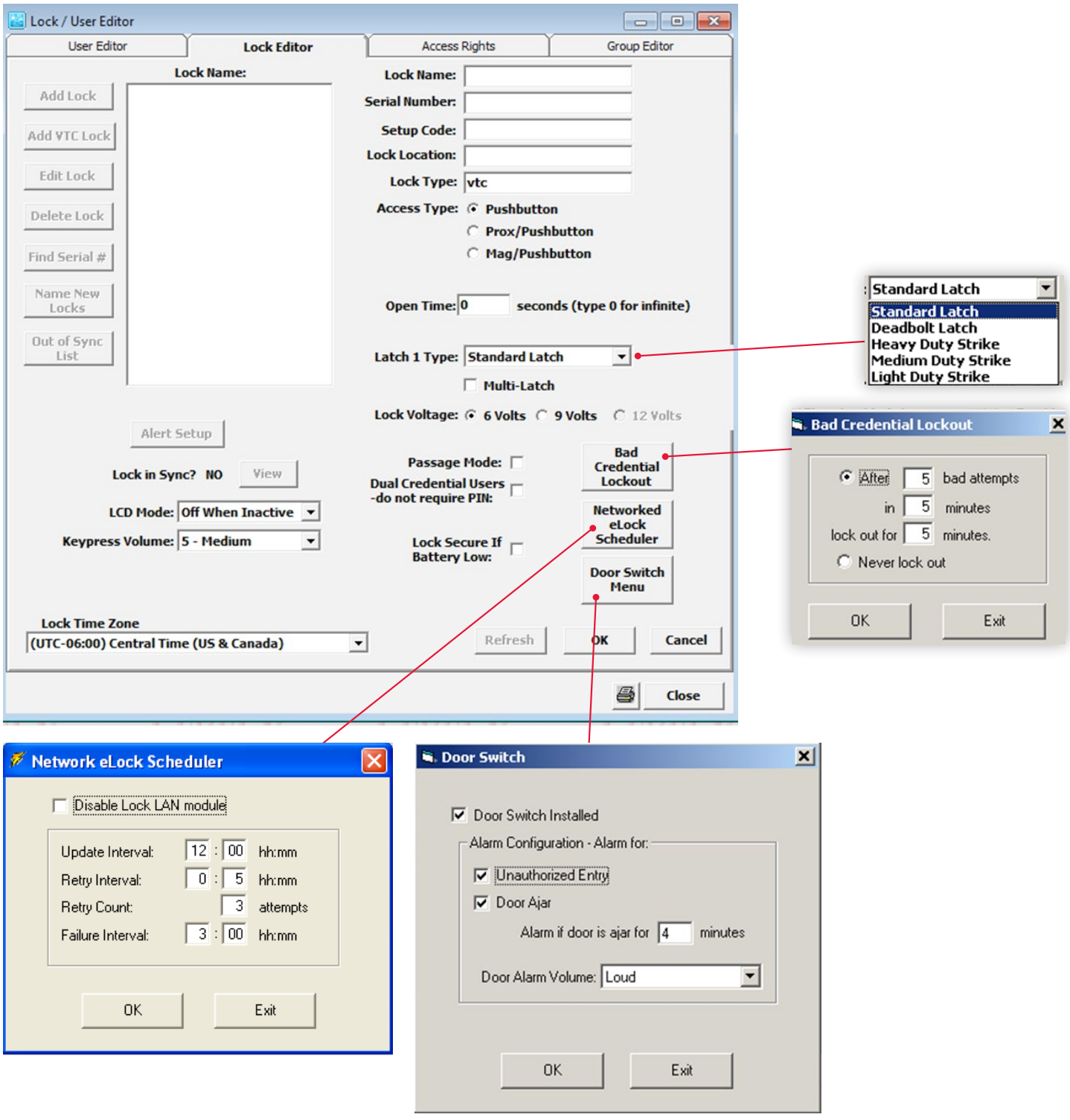
LOCK EDITOR

The **Lock Editor** tab is used to add, edit, or delete locks from the database.

TO ADD A NEW LOCK MANUALLY

1. Select **Lock/User Editor**. Select **Lock Editor**.
2. Select **Add VTC Lock** to create a new lock in the database.

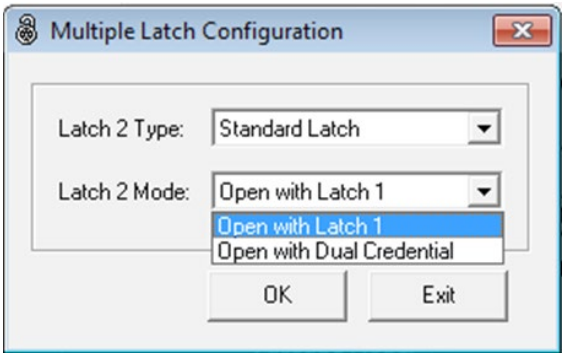
NOTE: the screen will change to the image shown below upon clicking "Add VTC Lock."



LOCK / USER EDITOR continued

Note: The Lock Editor shown here applies ONLY to VTC systems. See pages 15-19 for NTC systems.

3. Enter a name for the new lock being created. **Lock Name** must be between 4 and 14 characters in length including spaces.
4. Enter the **Lock Serial** and **Setup Code** numbers.
   - ➔ **The lock's serial and setup code numbers are on a sticker included with the lock.**
5. If the application (cart, cabinet, enclosure, etc) on which the eLock is installed comes with special LockView instructions, enter the name of the manufacturer of the application into the box next to Manufacturer. Entering this manufacturer name will open up additional settings for the application.
6. Choose the **Pushbutton, Prox/Pushbutton, Mag/Pushbutton** (under access type) if the lock being entered is provided with one of these card readers. **NOTE**: It is not possible to edit a lock's access type. If the lock's access type needs to be changed, the lock must be ***deleted*** and ***recreated*** with the appropriate card reader selected. **Prox/Pushbutton** corresponds to HID Prox/keypad and HID iCLASS/keypad.
7. Enter the number of seconds **Open Time (sec)** to program how long the lock will remain open before automatically re-locking. Entering 0 will keep the lock open indefinitely.
8. Select the type of latch in the **Latch 1 Type** box.
   NOTE: VTC users should choose "Standard Latch." Any other selection will cause undesired operation.
   - ➔ **Standard Latch** is the standard die cast CompX eLatch that is typically installed in the retrofit eLock product.
   - ➔ **Deadbolt Latch** is a specially equipped CompX eLatch that has been constructed to push the bolt out upon locking. There is no spring return.
   - ➔ If a 12V door strike is connected, select the smallest size strike (**Heavy Duty**, **Medium Duty** or **Light Duty**) that will keep the internal solenoid pulled in after it opens. This will conserve battery life.
   - ➔ If a 12V door strike is connected the **Lock Voltage** setting must be **12V**.
9. If the eLock is equipped with two latches, select the multi-latch config button. This will allow the type of multi-latch to be selected along with the multi-latch's behavior.



Latch 2 Type can be set to any of the styles available for **Latch 1 Type**. There are two settings for **Latch 2 Mode**: **Open with Latch1** and **Open with Dual Credential**. If **Open with Latch1** is selected, latch 2 will open simultaneously with latch 1. If **Open with Dual Credential** is selected, latch 1 will open with the first credential of a dual credential user and latch 2 will open with the second credential of that dual credential user. **NOTE**: All second credentials must be a 4 to 14 digit PIN.

10. Select the **Lock Voltage** box for the appropriate voltage for the eLock. The lock voltage selection will determine the low battery indicator threshold. If it is set incorrectly, the low battery indicator will not operate properly. **NOTE: VTC users should choose 9V.**
11. **Passage Mode** allows the eLatch to change its state (lock/unlock) after a valid credential is presented. To enter passage mode, press "ENTER" (at the eLock) after presenting a valid credential. Once the eLock is held open in passage mode, closing the eLock requires the acceptance of a valid credential.
12. Select **Dual Credential Users do not Require PIN** for this eLock in order to allow all dual credential users access with only their primary credential. **NOTE**: This will result in a reduction of security, as dual credential users will no longer be required to present both of their credentials.
13. If the eLock is equipped with temperature monitoring, check the box adjacent to **Temperature Lock**. Temperature will appear after clicking OK and allow access to additional temperature monitoring settings. **NOTE: VTC users should not choose this selection.**

LOCK / USER EDITOR continued

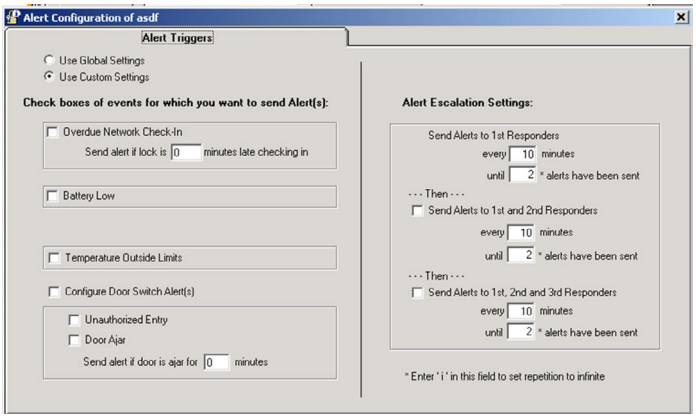
Note: The Lock Editor shown here applies ONLY to VTC systems. See pages 15-19 for NTC systems.

14. Select **Lock Secure If Battery Low** to prevent access to an eLock if the battery is low. If this box is checked, the eLock will NOT open if the battery is low. Replacing the battery will allow normal use.
15. To conserve battery, the LCD screen on the eLock can be set to turn "off" when not in use. **LCD Mode**; **Off When Inactive** is the default. Select **Always On** if the LCD is to remain on at all times.
16. The volume of the beeps that are heard when the buttons are pressed at the eLock is adjustable under **Keypress Volume**. Choose **0** to **9**: 0 is **Off** and 9 is **Loud**.
17. The local time zone on which the eLock is installed can be selected in **Lock Time Zone**. Provided the eLock is networked and in the event that the server resides in a different time zone, this feature ensures the correct time is recorded in the LockView audit trail
18. **Bad Credential Lockout** allows the operator to restrict access to a lock if multiple invalid attempts are made; default is **Never Lockout**. Click bad credential lockout to adjust.
    There are three adjustments:
    a) **After __ bad attempts**
    b) **In __ minutes**
    c) **Lockout for __ minutes**
    For example, after 5 bad attempts in 5 minutes, lockout for 5 minutes.
19. If the lock is provided with an Ethernet or 802.11 module, choose how often the lock will check for updates to the database buy clicking **Networked eLock Scheduler**. This will pop up a window. **NOTE**: If the lock does not have a LAN module, choose **Disable Lock LAN Module.**
    a. **Update Interval**- How often the lock will turn on the LAN module and check the network database for updates (enter in HH:MM format). **Default is 12 hours**.
    b. **Retry Interval**- If the networked lock was unable to connect to the database through the network, enter the amount of time before it retries. (enter in HH:MM format). **Default is five minutes**.
    c. **Retry Count**- If the networked lock fails to connect to the database upon retry, the lock will continue to retry the number of times in the "retry count." **Default is five attempts**.
    d. **Failure Interval**: If every attempt to connect to the database under the **Retry Count** is unsuccessful, **Failure Interval** is the amount of time the lock will wait before starting the **Retry Interval** again. (Enter in HH:MM format.) **Default is one hour**.

    NOTE*: Each time the lock turns on the LAN module to check the database for updates, a significant amount of energy is drained from the battery, reducing battery life.*

20. If a door switch is installed, click **Door Switch Menu** to open the door switch submenu. The eLock can be set to alarm if the door switch opens without a valid credential (**Unauthorized Entry**) and/or it can be set to alarm if the door has been left open for a programmable amount of time (**Door Ajar**). The alarm volume can also be set to **Off**/**Soft**/**Medium**/**Loud**.

21. GLOBAL LOCK SETTINGS
    If the new eLock will be part of the Notifier system (See **Notifier** page 43) click **Alert Setup** to enter the proper settings.


Alert Configuration of asdf
Alert Triggers
Use Global Settings
Use Custom Settings
Check boxes of events for which you want to send Alert(s):
Overdue Network Check-In
Send alert if lock is 0 minutes late checking in
Battery Low
Temperature Outside Limits
Configure Door Switch Alert(s)
Unauthorized Entry
Door Ajar
Send alert if door is ajar for 0 minutes
Alert Escalation Settings:
Send Alerts to 1st Responders
every 10 minutes
until 2 * alerts have been sent
- - - Then - - -
Send Alerts to 1st and 2nd Responders
every 10 minutes
until 2 * alerts have been sent
- - - Then - - -
Send Alerts to 1st, 2nd and 3rd Responders
every 10 minutes
until 2 * alerts have been sent
* Enter '-' in this field to set repetition to infinite

LOCK / USER EDITOR continued

Note: The Lock Editor shown here applies ONLY to VTC systems. See pages 15-19 for NTC systems.

SETUP THE ALERT TRIGGERS

1. Click **Use Global Settings** or **Use Custom Settings**. **Global Settings** will allow this eLock to follow the **Global Settings** that are programmed under **Notifier; Global Lock Settings**. **Global Settings** allows the LockView Operator to manage multiple similar eLocks simultaneously without having to adjust each one individually. Click Use **Custom Settings** if this eLock will have different alarming settings from those that follow global settings.

   If **Use Custom Settings** is selected:

2. Choose the eLock alert events for which notification is desired.
   - Select **Overdue Network Check-In** to send an alert(s) if an eLock has missed the scheduled network update (see **Lock/ User Editor; Lock Editor Network eLock Scheduler** on page 22) for which the amount of time past due is programmable.
   - Select **Battery Low** to send an alert(s) if the battery power drops too low.
   - If the eLock is a temperature monitoring eLock, **Temperature Outside of Limits** selection will appear. This setting will send an alert(s) if the eLock has 1) temperature alarming enabled, 2) the current temperature is outside of the high/low limits and 3) the temperature has been outside of the specified limits for a time exceeding the **Alarm Delay** time.
   - If **Door Switch Installed** was selected in the **Lock Editor**; **Door Switch** menu, the **Configure Door Switch Alerts** selection will appear. This alert can be sent for two types of **Door Switch Alerts**. **Unauthorized Entry** will send an alert(s) if the door switch opens at a time not immediately following the presentation of a valid credential. **Door Ajar** will send an alert(s) if the door has been open for a programmable amount of time; past the standard eLock open time (see **Lock Editor-Door Switch Menu** on page 22).

3. **Alert Escalation Settings** allows the LockView Operator to set up a schedule for how often and how many alert(s) will be sent to the Responder(s).

   - Enter how often and how many alert(s) will be sent to the 1st Responder(s) before escalating to the 2nd Responder(s).
   - Enter how often and how many alert(s) will be sent to the 2nd Responder(s) before escalating to the 3rd Responder(s).
   - Enter how often and how many alert(s) will be sent to the 3rd Responder(s).

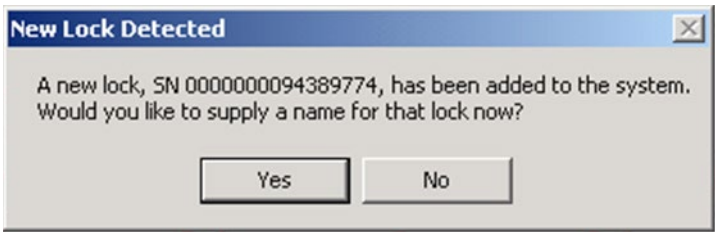
   NOTE: *Entering an "i" in the number of alerts field will force an infinite number of alerts.*

4. Click **Save** when done.

   NOTE: *The lock's internal memory must match the database for every setting noted above. The status of the lock setting VS database setting is shown adjacent to* ***Lock in Sync? Yes/No.*** *If the lock and the database are NOT in sync, the* ***VIEW*** *button will appear. This button will open the* ***Lock Settings*** *tab in* ***Read/Write Lock.***

TO ADD A NEW LOCK AUTOMATICALLY

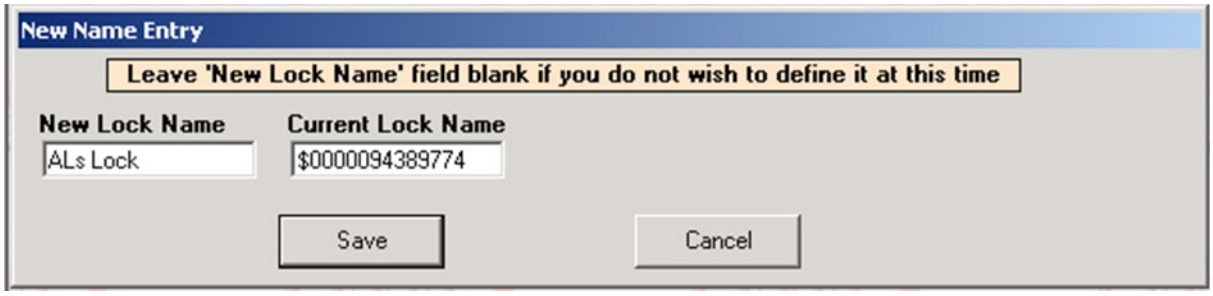
1. Press and hold "CLEAR" on the keypad. "**ENTER SETUP CODE**" will appear.
2. Enter the setup code that was provided on the sticker set with the lock into the keypad.
3. Connect a USB cable from the computer to the lock. If a network module (802.11 or Ethernet) is being used and it is setup and properly configured, press the "NETWORK" button on the keypad to initiate a manual update.
4. Within a few seconds, the following window will appear in LockView. SNXXXX is the serial number of the lock being added.


New Lock Detected
A new lock, SN 0000000094389774, has been added to the system.
Would you like to supply a name for that lock now?
Yes
No

LOCK / USER EDITOR continued

Note: The Lock Editor shown here applies ONLY to VTC systems. See pages 15-19 for NTC systems.

5. Click **Yes.**
6. Enter the **New Lock Name**. The lock and all of the settings will be loaded into the database.



TO EDIT AN EXISTING LOCK

1. Select **Lock/User Editor**. Select **Lock Editor**.
2. Highlight **Lock Name** and select **Edit Lock**. **NOTE**: lock **Access Type** cannot be edited.
3. Select **OK** when done.

NOTE: *The lock's internal memory must match the database for: Access Type, Open Time, Passage Mode, Dual Credential Users do not Require PIN, Keypress Volume, Bad Credential Lockout, LCD Mode, Lock Secure If Battery Low, Lock Voltage, Door Switch Menu, latch number and type. To compare the lock settings information and database information, go to the* ***Lock Settings*** *tab under* ***Read/Write Lock*** *and update as necessary.*

4. Select **Close**.

TO DELETE A LOCK

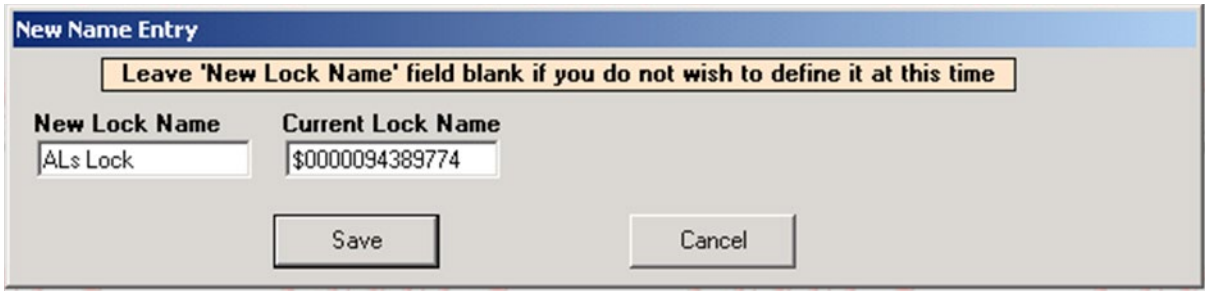
1. Select **Lock/User Editor**. Select **Lock Editor**.

NOTE: *Before deleting a lock, it is recommended to remove all access rights to the lock from all users. This ensures the lock is deleted and will not be accidentally reinstated.*

2. Highlight lock name and select **Delete Lock**.
3. Select **Close** to close **Lock Editor**.

TO NAME A NEW LOCK

If a lock was automatically entered into the database and has not been given a proper name; the lock name will appear as $xxxxxxx in the list of locks in the **Lock Editor**, "xxxxxxx" represents the serial number of the lock. To give the locks a proper name, click **Name New Locks.**



OUT OF SYNC LIST

Clicking the **Out of Sync** button will open a window that shows the list of locks that are not "in sync" with the database (lock settings or current users)

LOCK / USER EDITOR continued

ACCESS RIGHTS

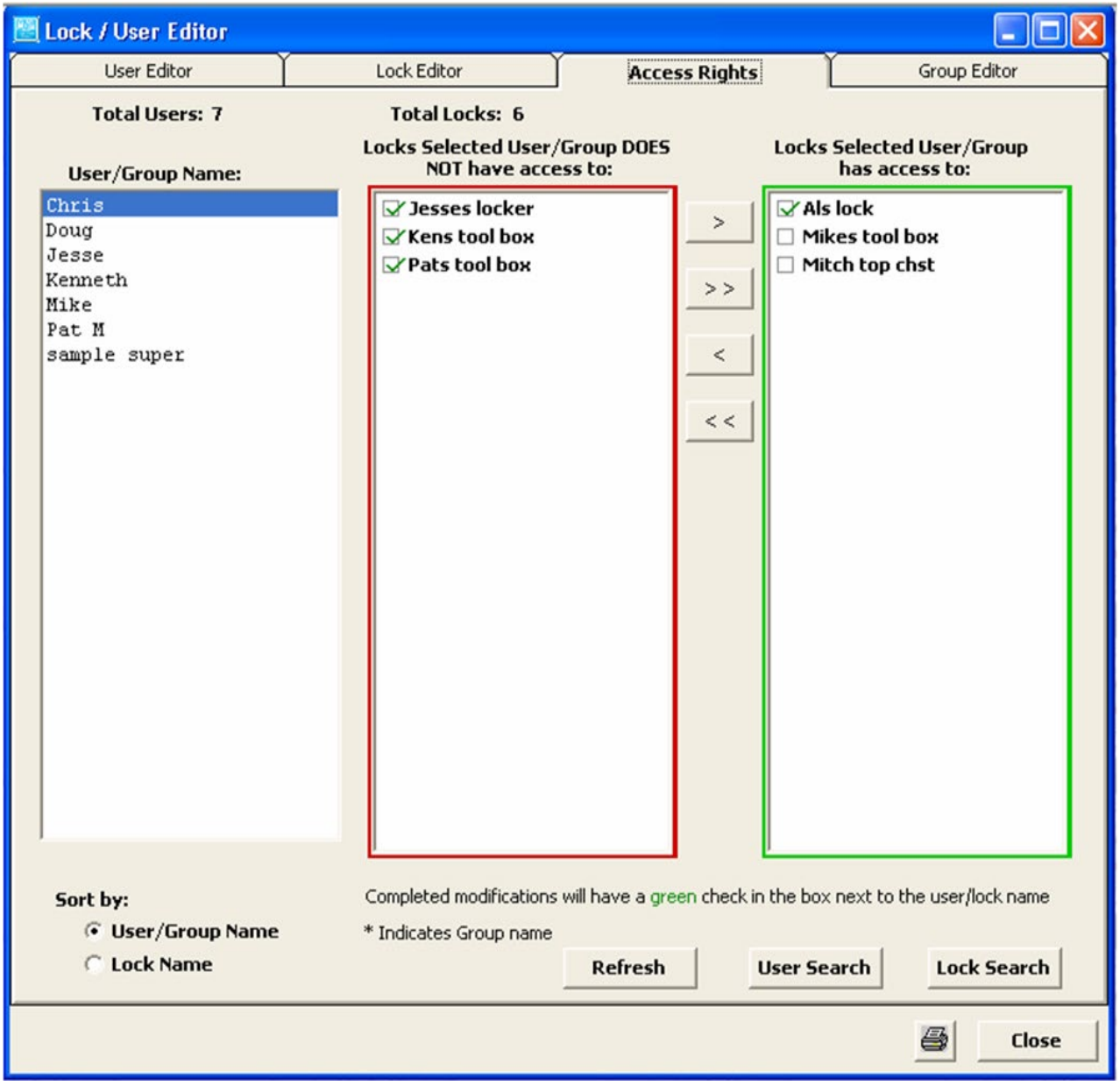
Access Rights is used to choose which locks users can have access to in the database. Each lock is limited to a total of 999 users.

1. Select **Access Rights** from the **Lock/User Editor** window.

   NOTE: *Select **User/Group Name** or **Lock Name** in the bottom left corner under **Sort by** to view access rights organized by user/group name or lock name/group. In steps 2-4, the window is set for Sort by: User/Group Name.*

2. Select the user/group whose access rights will be modified.
   - ➔ All locks in the left column are locks to which the selected user/group does not have access.
   - ➔ All locks in the right column are locks to which the selected user/group has access.

   NOTE: *An unchecked box in the adjacent entry represents information that has not yet been uploaded into the lock.*



LOCK / USER EDITOR continued

3. To change access rights for a single lock, select lock from the list and:
   - ➔ Press the appropriate single arrow button between the two columns, or
   - ➔ Double click on the lock name.
4. To change access rights for all the listed locks:
   - ➔ Switch one lock at a time (refer to step 3), or
   - ➔ Press the appropriate double arrow button between the two columns.

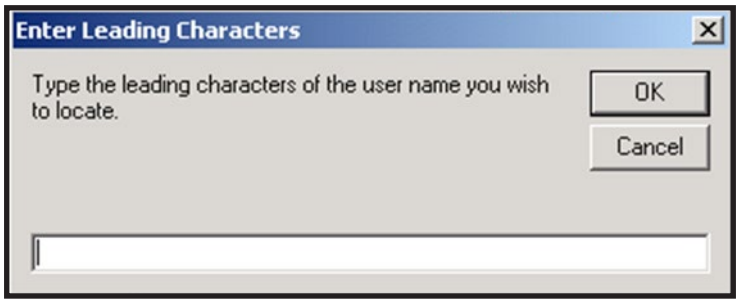
NOTE: *Changing a position in **Access Rights** only changes the computer database. The contents of the lock do not automatically change. See **READ/WRITE LOCK** for instructions on updating the lock database.*

NOTE: *If there is a change to a user's status, i.e. Supervisor Level, Time Based Access, Passage Mode, etc. the box on the right will be unchecked. A Write Changes operation will need to be completed to update the lock.*

5. When viewing users/groups, the group name will be followed by an asterisk (*) along with the number of members of the group in parentheses, for example **(4)** indicates four members. When adding groups, each group member will use one memory slot in the lock.

   - ➔ Access rights can also be sorted according to the lock name. If organized by lock name, refer to steps 2-4 but substitute lock access rights for users access rights.

6. If a user/group/lock cannot be found, click **User Search** or **Lock Search.** Click **OK** after the leading characters of the user/group/lock name have been entered.



GROUP EDITOR

The **Group Editor** tab is used to add, edit, or delete groups from the computer database. This option makes it easier to add or delete groups of users from a lock. Users in a group will all have the same time-based access to locks, as well as common access rights.

TO ADD A NEW GROUP

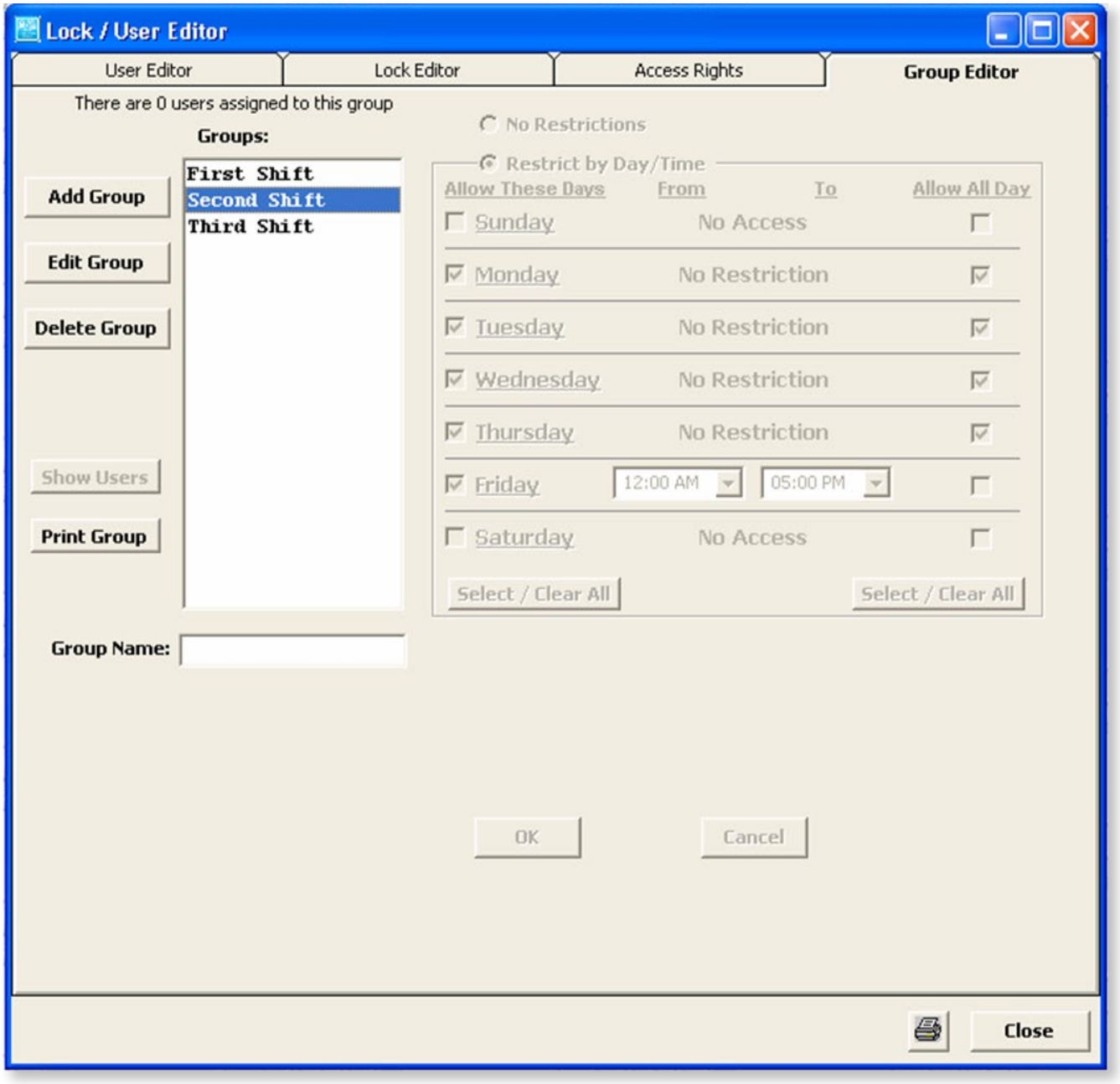
1. Select the **Lock/User Editor** window. Select the **Group Editor** tab.
2. Select **Add Group** to create a new group in the computer database.
3. Enter the new group's name.
4. If the new group has no restrictions, check the **No Restrictions** box.
5. If the new group has restricted access to locks, check the days the group is not restricted.

LOCK / USER EDITOR continued

6. Fill in the time slots the new group can access the locks, or check the **All Day** box if the group has 24 hour access. When filling in time slots, LockView® will automatically wrap a day. (Example: 11 p.m. Monday - 7 a.m. Tuesday.)
7. Select **OK** when done.
8. Select **Close** to close the **Group Editor** tab.

TO EDIT A NEW GROUP

1. Select the **Lock/User Editor** window. Select the **Group Editor** tab.
2. Select group name and then select **Edit Group** to edit the group's restriction information.
3. Select **OK** when done.
4. Select **Close** to close the **Group Editor** tab.



LOCK / USER EDITOR continued

TO DELETE A GROUP

1. Select the **Lock/User Editor** window.

   NOTE: *If you delete a restriction group, all users assigned to it will be set to "No Access."*

2. Select group name and then select **Delete Group** to delete an existing user from the local computer database.
3. Select OK to close the **Group Editor** tab.

PRINT GROUP

To print the names of the members of a group(s) AND the locks to which they have access, click the **Print Group** tab.

SHOW USERS

Clicking the Show Users button will pop up a list of all users currently assigned to a highlighted group.

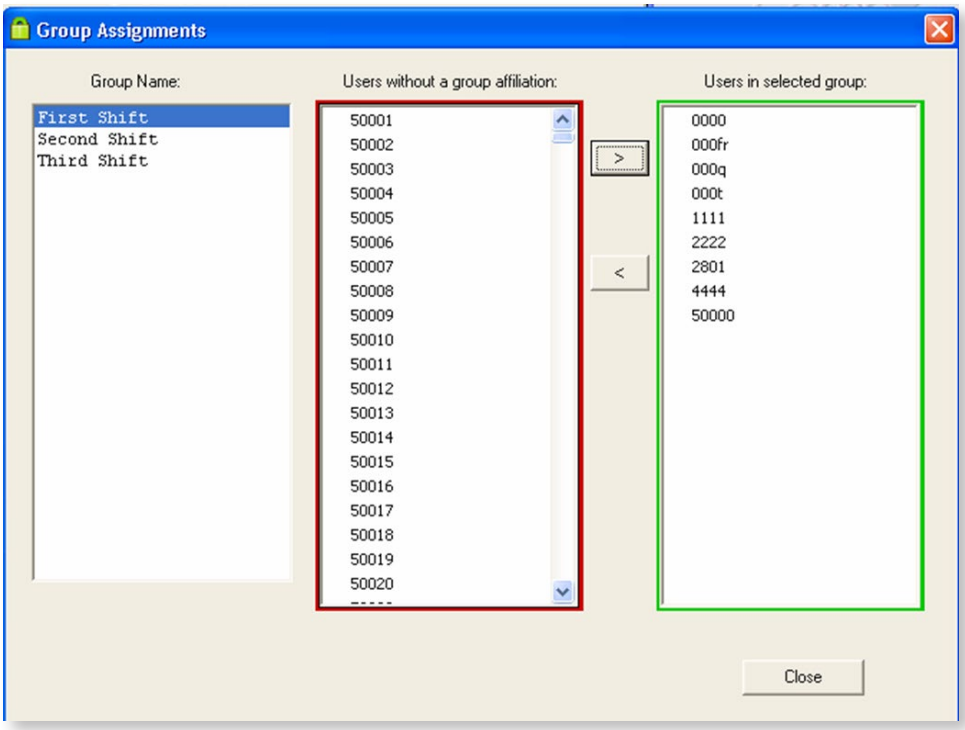
Read/Write Lock contains four (4) tabs that allow the Operator to view the database of a lock and download the audit trail from a lock.

USER/GROUP ASSIGNMENT

1. Select **User / Group Assignment** to open up the **Group Assignments** window. The name of the group(s) appear in the left column.
2. Click to highlight the name of the group of interest.
3. The middle column (outlined in red) lists all users who do not have an affiliation to the selected group. The right column (outlined in green) lists all users who are affiliated with the selected group.
4. Click to highlight the user(s) to be manipulated and click the **<** or **>** button to shift the user(s) into the desired columns.

   NOTE: *Ctrl + click or Shift + click can be used to highlight multiple users.*

5. Click **Close** button when done.

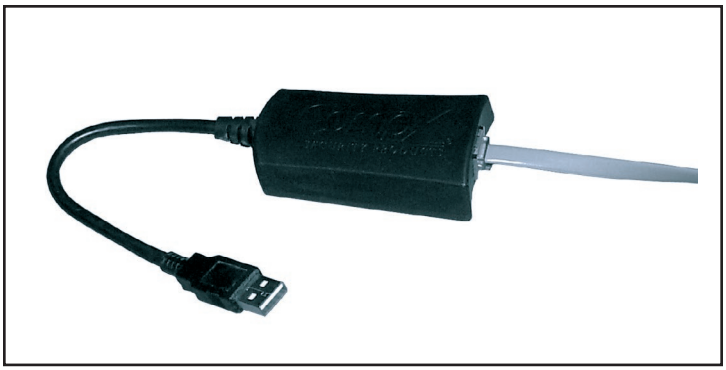


READ / WRITE LOCK

Read/Write Lock contains four (4) tabs that allow the Operator to view the database of a lock and download the audit trail from a lock.

CONNECTION

Connection allows the Operator to view a lock's memory content — either virtually (with a networked connection) or in real time with a USB dongle connection.



TO CONNECT TO A LOCK:

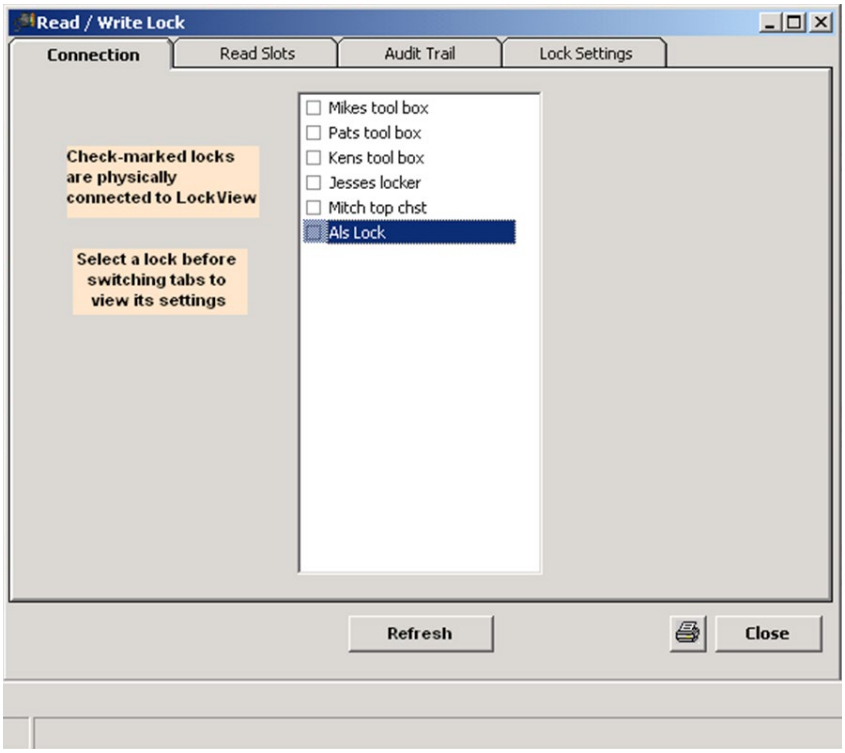
1. Select **Read/Write Lock**. If the **Read/Write Lock** window is already open, make sure the **Connection** tab is open.
2. Connect the 6 wire RJ11 cable from the lock to the LockView® USB adapter if real time slot reading is desired.
3. The connection icon should show a **RED** background.

When the USB dongle is inserted and and LockView is properly communicating with the dongle, the connection icon should show a **GREEN** background.

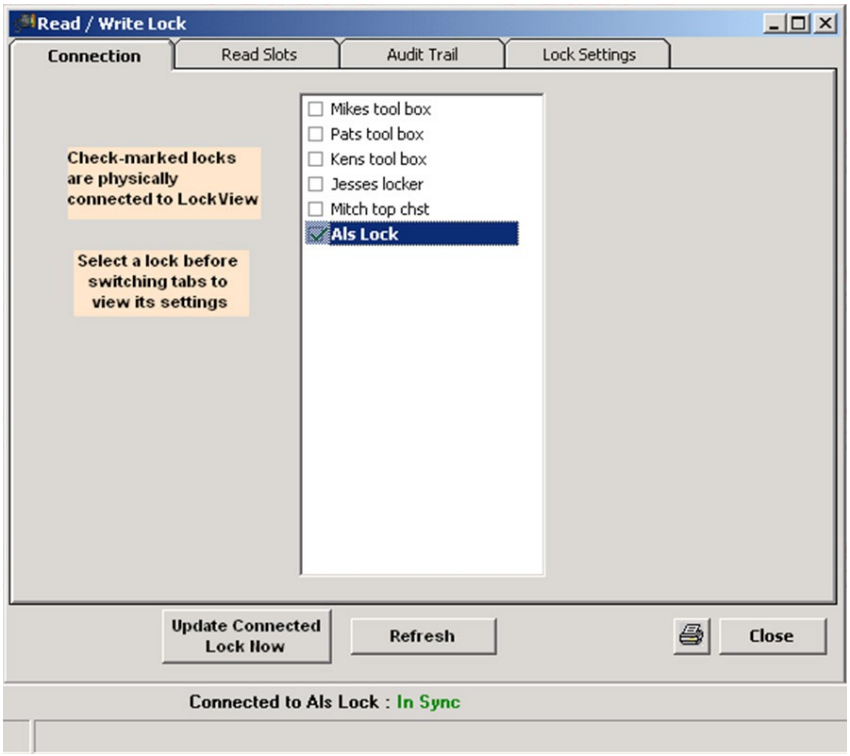
If the connection background does not change to green, the dongle drivers are not properly loaded. Visit **compx.com** to download new dongle drivers or contact technical support.

READ / WRITE LOCK continued

4. The **Read/Write Lock** screen is shown below.



5. Insert the other end of the 6 – wire RJ11 cable into the lock. After a few seconds, the screen should look similar to the figure below, with the lock name to which the RJ11 cable is connected being highlighted with a check appearing the box next to it. Further, the status bar will now say **Connected to:** ***lock name*** where lock name is the name of the connected lock.



READ / WRITE LOCK continued

READ SLOTS

Read Slots allows the Operator to view the slots assigned to users in the database along with the actual contents of the slots in the lock. If the computer database and the lock contents for a numbered slot do not match, the information in the corresponding slots will be displayed in different colors.

1. Highlight the lock to view in the **Connection** tab of the **Read/Write Lock** menu.
2. Select **Read Slots**.

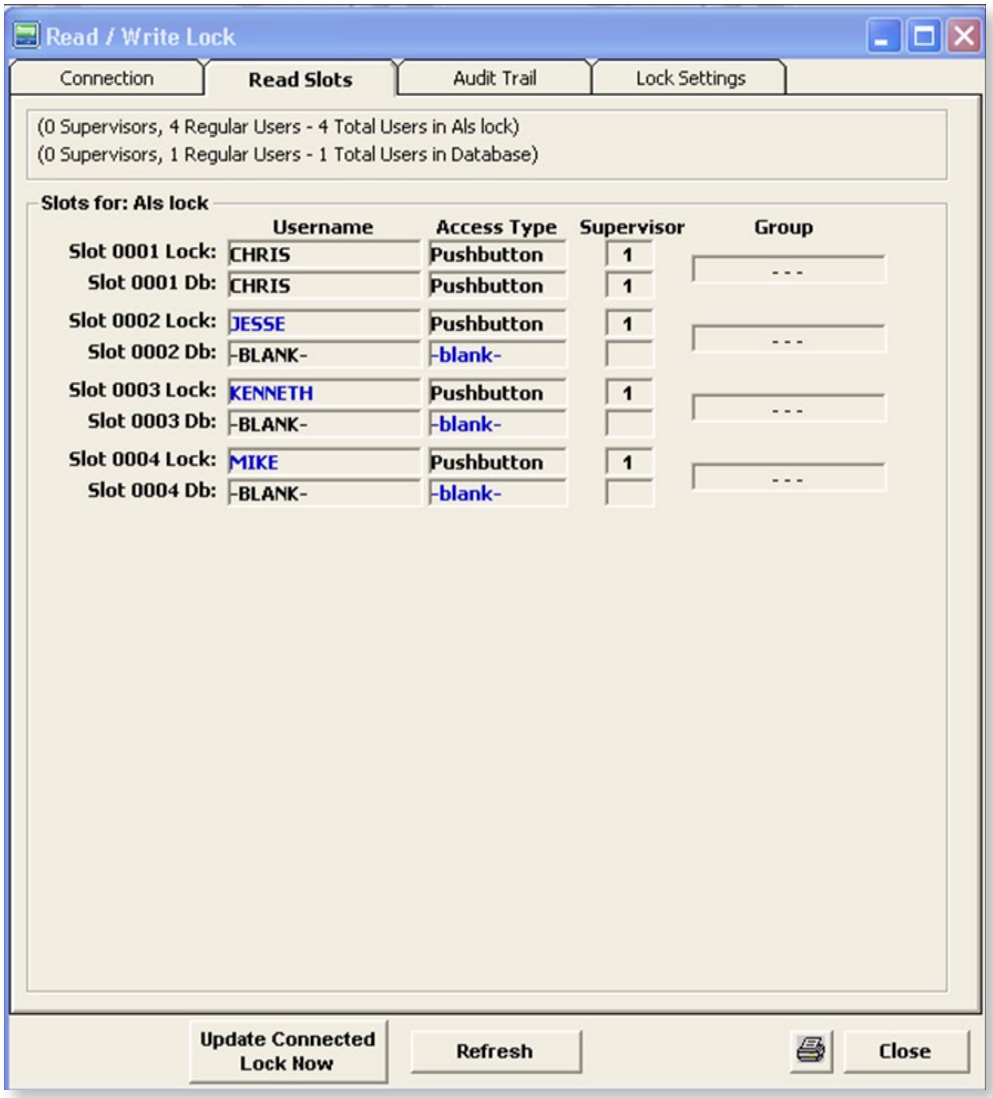
LOCK DATABASE INFORMATION "LOCK"

- User name
- Access type
- Slot number
- Supervisor rights level
- Group Membership

COMPUTER DATABASE INFORMATION "Db"

- User name
- Access type
- Slot number
- Supervisor rights level
- Group Membership

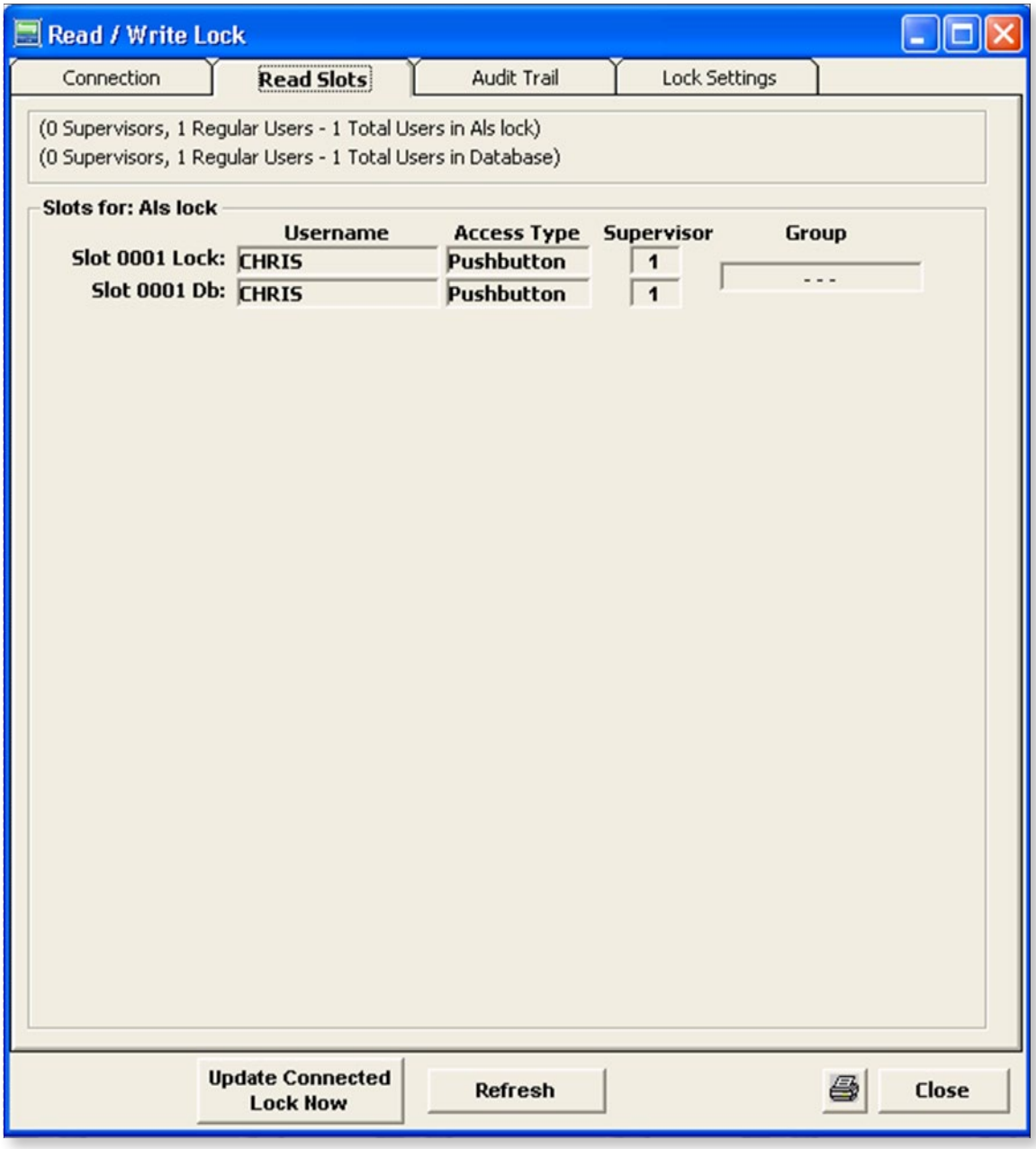
This report also shows if information in the slot database of the lock differs from the slot in the computer database. This is illustrated with blue text, and black text. If the entry in the computer database is in orange, the users information (supervisor level, passage mode status, dual credential status, time based access status, messages, slave access) in the database has been modified and will need to be updated within the lock's database.


Read / Write Lock
Connection
Read Slots
Audit Trail
Lock Settings
(0 Supervisors, 4 Regular Users - 4 Total Users in Als lock)
(0 Supervisors, 1 Regular Users - 1 Total Users in Database)
Slots for: Als lock
Username
Access Type
Supervisor
Group
Slot 0001 Lock: CHRIS Pushbutton 1 ---
Slot 0001 Db: CHRIS Pushbutton 1
Slot 0002 Lock: JESSE Pushbutton 1 ---
Slot 0002 Db: -BLANK- -blank-
Slot 0003 Lock: KENNETH Pushbutton 1 ---
Slot 0003 Db: -BLANK- -blank-
Slot 0004 Lock: MIKE Pushbutton 1 ---
Slot 0004 Db: -BLANK- -blank-
Update Connected Lock Now
Refresh
Close

This Read Slots screen shows:

- Four slot assignments for the computer database and a lock titled "Als Lock"
- Slots 0002, 0003, and 0004 of the computer database do not match the lock's database.

READ / WRITE LOCK continued



The **Update Connected Lock Now** button was pressed or the update occurred automatically. The computer database and lock database now match.

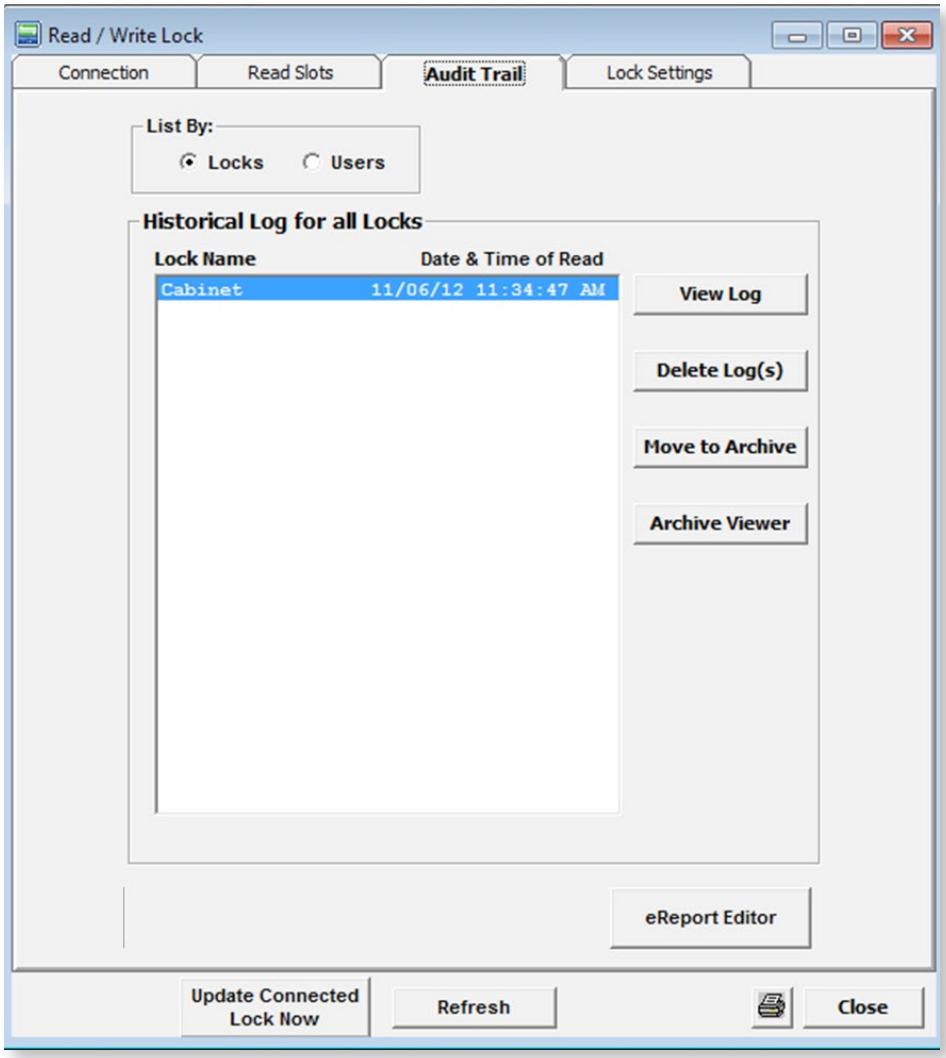
NOTE: *The Update Connected Lock Now button does not appear in a network connection. The databases will automatically sync upon a network connection.*

READ / WRITE LOCK continued

AUDIT TRAIL

Audit Trail allows the Operator to view the audit trail of a lock or a user. A "lock" audit trail is a log of a lock's past operation. These logs include the name of a user attempting to gain access, name of the lock being accessed, what type of credential is being used, and the date and time of attempted access. A "user" audit trail is a log of a user's past operation. These logs include the name of a user, name of the locks being accessed by the user, what type of credential is being used, and the date and time of attempted access.

Choose which type of audit trail is desired by pressing the locks or users button under **List by**.



1. Select **Audit Trail** from **Read/Write Lock** window.
2. Select the lock whose audit trail is to be viewed.
3. Select **View Log**.

LOG INFORMATION INCLUDES:

- Name of the lock
- Name of the user that attempted access to the lock (if the database has a record for that credential)
- The credential type that was used by the user
- Date and time of attempted access
- Activity detail, noted under "status"

READ / WRITE LOCK continued

FULL STATUS LIST:

Latch opened
This is an indication of a valid credential being shown, and the lock successfully opening.

***Drawer opened**
This is an indication of one of the drawer switches opening (optional hardware required and **Drawer Alarm** must be activated in the **Lock Editor**, **OR** the drawer alarm must be activated on a slave lock). May also be prefaced with a slave number (*), if the drawer alarm on the slave lock is activated.

***Tilt detected**
This is an indication an of the tilt alarm sensor sounding. **Tilt Sensitivity** in the **Lock Editor** must not be set to 0, **OR** the tilt alarm must be activated on a slave lock. May also be prefaced with a slave number (*), if the tilt alarm on the slave lock is activated.

Latch closed
This is an indication of the lock closing, either by a valid credential being shown, the **lock** button being pressed on the access panel or the **Open Time** timing out.

***Drawer closed**
This is an indication of all of the drawer switches closing (optional hardware required and **Drawer Alarm** must be activated in the **Lock Editor OR** the drawer alarm must be activated on a slave lock). May also be prefaced with a slave number (*), if the drawer alarm on the slave lock is activated.

***Tilt cleared**
This is an indication of the clearing (turning off) of the tilt alarm. **Tilt Sensitivity** in the **Lock Editor** must not be set to 0, **OR** the tilt alarm must be activated on a slave lock. May also be prefaced with a slave number (*), if the tilt alarm on the slave lock is activated.

Reboot FW version XX
This is an indication of the microprocessor restarting the firmware, firmware version is noted.

Inventory acceptable ...
This is an indication that a visual inventory of the toolbox was taken with acceptable results. May be followed by up to 14 numeric digits entered by the person performing the visual inventory.

Inventory missing items ...
This is an indication that a visual inventory of the toolbox was taken with unacceptable results. May be followed by up to 14 numeric digits entered by the person performing the visual inventory.

Time change: Prior to change
Time change: After change
A supervisor has changed the time at the lock. "Prior to change" was the time that the lock was set when the time was changed. "After change" is the time to which the lock was set.

Access Denied- 2nd PIN mismatch.
This is an indication that access was denied to a dual credential user or supervisor due to second credential being incorrect.

Access granted on 2nd PIN.
This is an indication that access was granted to a dual credential user or supervisor.

READ / WRITE LOCK continued

Supervisor Mode granted on 2nd PIN.
This is an indication that the programming screens were accessed by a supervisor with dual credential.

Access Denied- No rights.
A credential was presented which was not recognized by the lock.

Access Denied- Lock was in lockout mode
This is an indication that access was denied to a user or supervisor due to the lock being locked out.

Access Denied- Time restriction.
This is an indication that access was denied to a user or supervisor due to time restrictions .

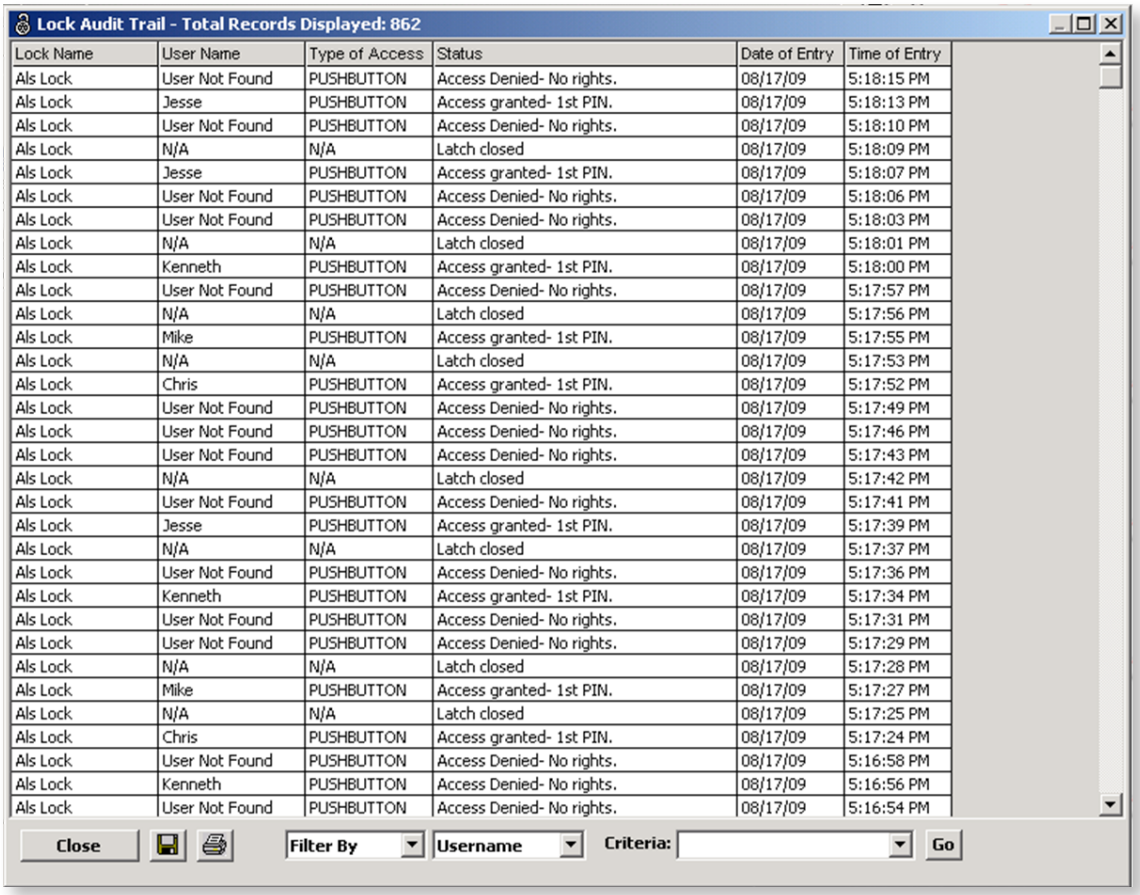
Access Pending- Await 2nd PIN.
This is an indication that the primary credential was accepted for a dual credential user or supervisor.

Access granted- 1st PIN.
This is an indication that access was granted to a dual credential user or supervisor on the first pin (**Dual Credential Users do not Require Pin** must be selected in the **Lock Editor**)

Supervisor Mode granted on 1st PIN.
This is an indication that the programming screens were accessed by a supervisor.

To view an older audit trail entry, select a historical audit trail log file and press the **View Log** button.

5. The tool bar at the bottom of the audit trail display allows the Operator to **Close, Print, Save** to an external text file or csv file, filter or sort the audit trail log information.



Lock Name	User Name	Type of Access	Status	Date of Entry	Time of Entry
Als Lock	User Not Found	PUSHBUTTON	Access Denied- No rights.	08/17/09	5:18:15 PM
Als Lock	Jesse	PUSHBUTTON	Access granted- 1st PIN.	08/17/09	5:18:13 PM
Als Lock	User Not Found	PUSHBUTTON	Access Denied- No rights.	08/17/09	5:18:10 PM
Als Lock	N/A	N/A	Latch closed	08/17/09	5:18:09 PM
Als Lock	Jesse	PUSHBUTTON	Access granted- 1st PIN.	08/17/09	5:18:07 PM
Als Lock	User Not Found	PUSHBUTTON	Access Denied- No rights.	08/17/09	5:18:06 PM
Als Lock	User Not Found	PUSHBUTTON	Access Denied- No rights.	08/17/09	5:18:03 PM
Als Lock	N/A	N/A	Latch closed	08/17/09	5:18:01 PM
Als Lock	Kenneth	PUSHBUTTON	Access granted- 1st PIN.	08/17/09	5:18:00 PM
Als Lock	User Not Found	PUSHBUTTON	Access Denied- No rights.	08/17/09	5:17:57 PM
Als Lock	N/A	N/A	Latch closed	08/17/09	5:17:56 PM
Als Lock	Mike	PUSHBUTTON	Access granted- 1st PIN.	08/17/09	5:17:55 PM
Als Lock	N/A	N/A	Latch closed	08/17/09	5:17:53 PM
Als Lock	Chris	PUSHBUTTON	Access granted- 1st PIN.	08/17/09	5:17:52 PM
Als Lock	User Not Found	PUSHBUTTON	Access Denied- No rights.	08/17/09	5:17:49 PM
Als Lock	User Not Found	PUSHBUTTON	Access Denied- No rights.	08/17/09	5:17:46 PM
Als Lock	User Not Found	PUSHBUTTON	Access Denied- No rights.	08/17/09	5:17:43 PM
Als Lock	N/A	N/A	Latch closed	08/17/09	5:17:42 PM
Als Lock	User Not Found	PUSHBUTTON	Access Denied- No rights.	08/17/09	5:17:41 PM
Als Lock	Jesse	PUSHBUTTON	Access granted- 1st PIN.	08/17/09	5:17:39 PM
Als Lock	N/A	N/A	Latch closed	08/17/09	5:17:37 PM
Als Lock	User Not Found	PUSHBUTTON	Access Denied- No rights.	08/17/09	5:17:36 PM
Als Lock	Kenneth	PUSHBUTTON	Access granted- 1st PIN.	08/17/09	5:17:34 PM
Als Lock	User Not Found	PUSHBUTTON	Access Denied- No rights.	08/17/09	5:17:31 PM
Als Lock	User Not Found	PUSHBUTTON	Access Denied- No rights.	08/17/09	5:17:29 PM
Als Lock	N/A	N/A	Latch closed	08/17/09	5:17:28 PM
Als Lock	Mike	PUSHBUTTON	Access granted- 1st PIN.	08/17/09	5:17:27 PM
Als Lock	N/A	N/A	Latch closed	08/17/09	5:17:25 PM
Als Lock	Chris	PUSHBUTTON	Access granted- 1st PIN.	08/17/09	5:17:24 PM
Als Lock	User Not Found	PUSHBUTTON	Access Denied- No rights.	08/17/09	5:16:58 PM
Als Lock	Kenneth	PUSHBUTTON	Access Denied- No rights.	08/17/09	5:16:56 PM
Als Lock	User Not Found	PUSHBUTTON	Access Denied- No rights.	08/17/09	5:16:54 PM

READ / WRITE LOCK continued

THE AUDIT TRAIL LOG CAN BE FILTERED ACCORDING TO:

- User Name
- Type of Access

THE AUDIT TRAIL LOG CAN BE SORTED ACCORDING TO:

- User Name
- Type of Access
- Status
- Date and Time

6. Audit trails can be viewed, deleted and archived by selecting the appropriate button.

LOCK SETTINGS

Lock Settings allows the Operator to view the operating characteristics and parameters of the lock chosen in the **Connection** tab. The internal time of the lock and the computer are also displayed.

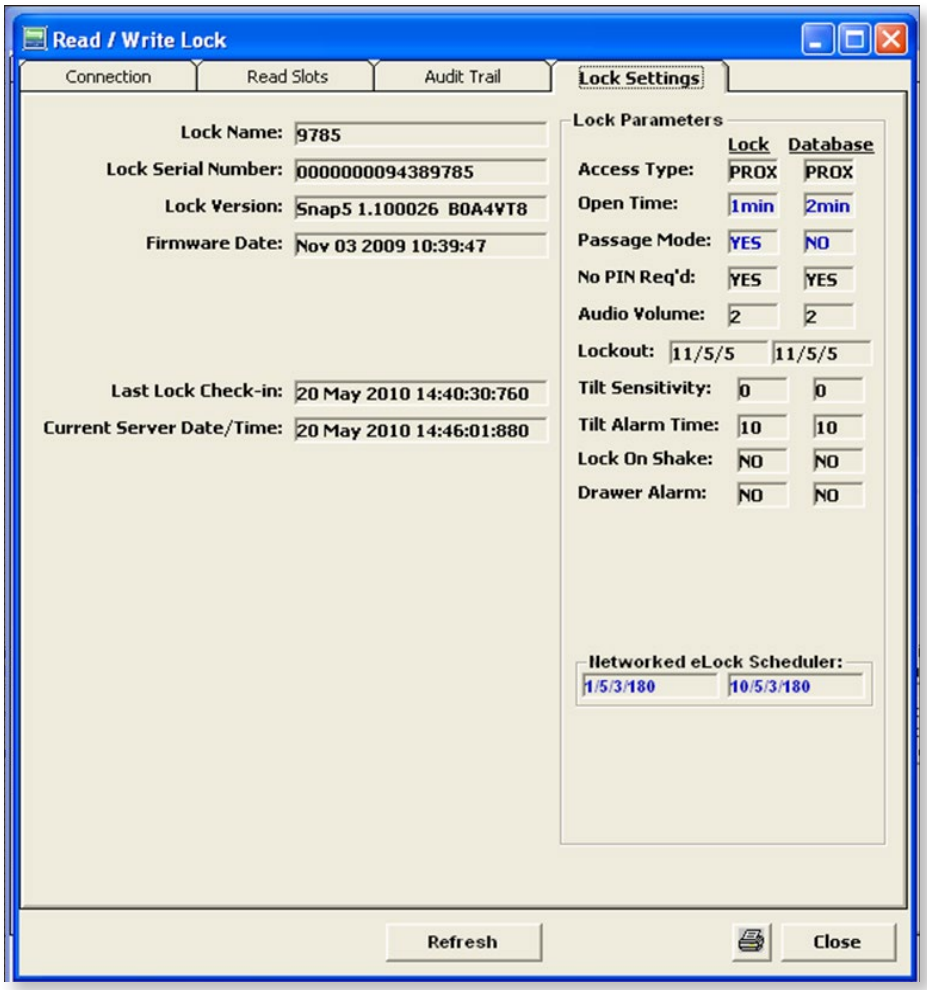
1. Choose desired lock to view under **Connection** tab.
2. Select **Lock Settings** from **Read/Write Lock**.
3. The lock and computer database characteristics and parameters are displayed.

VTC USERS: THE LOCK SETTINGS SCREEN LOOKS SLIGHTLY DIFFERENT ON VTC SYSTEMS, SHOWING VTC SPECIFIC FEATURES.

This screen shows:

- Lock Access Type
- Audio Volume
- Open Time
- Passage Mode
- No PIN Req'd (dual credential users do not require PIN)
- Tilt Sensitivity
- Tilt Alarm Time
- Lock On Shake
- Lockout
- Drawer Alarm
- LAN Times

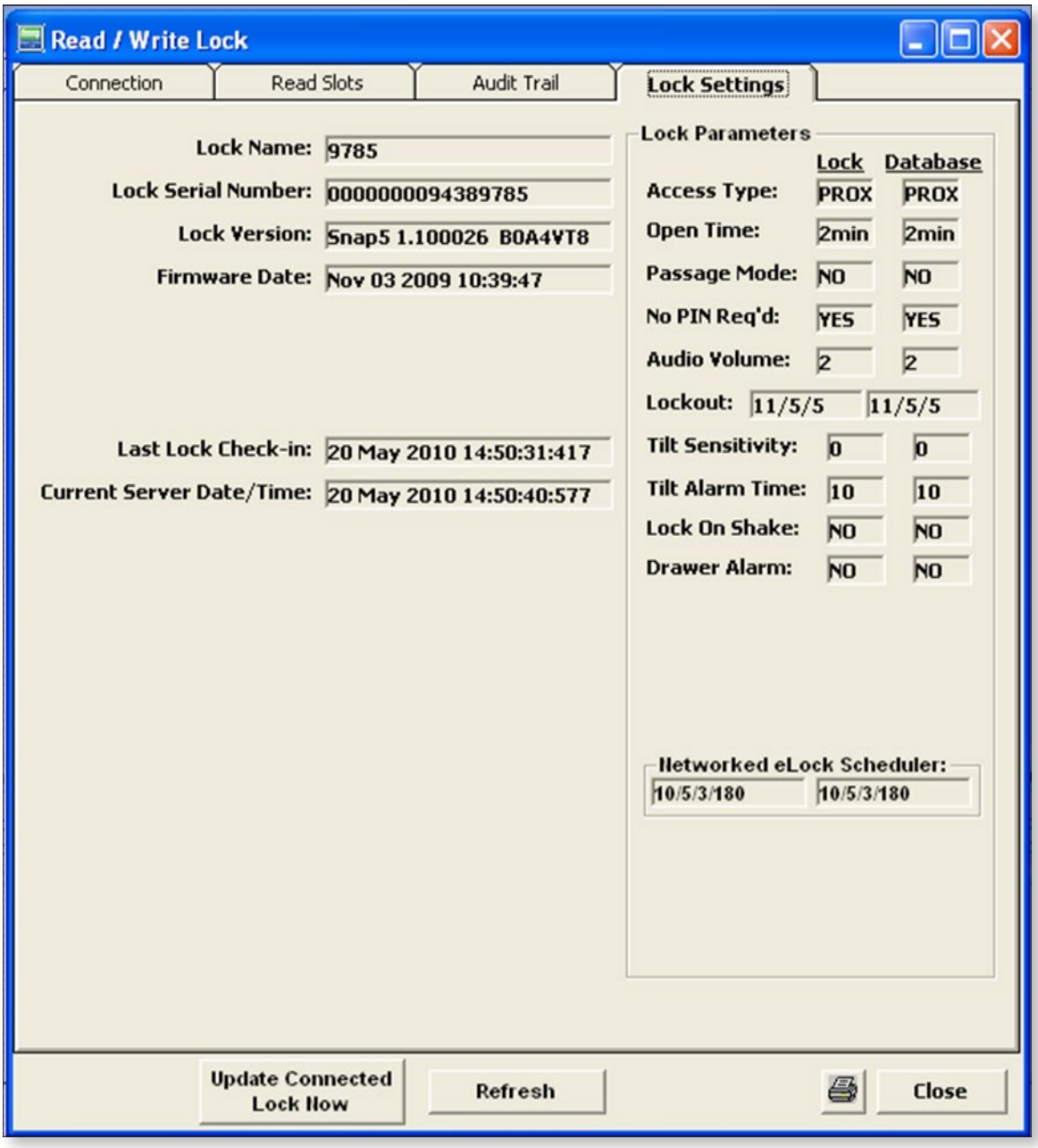
VTC USERS: THESE FEATURES WILL BE SLIGHTLY DIFFERENT ON VTC SYSTEMS.



READ / WRITE LOCK *continued*

This report also shows if information in the lock database differs from the information in the computer database. This is illustrated with blue text and black text. The Lock Parameter information can be found and/or edited by opening **Lock Editor**.

4. Click the **Refresh** button to compare lock data to computer database data.
5. **Update Connected Lock Now** permits a direct manipulation of the lock database. Click the **Update Connected Lock Now** button to match up the lock with the computer database.

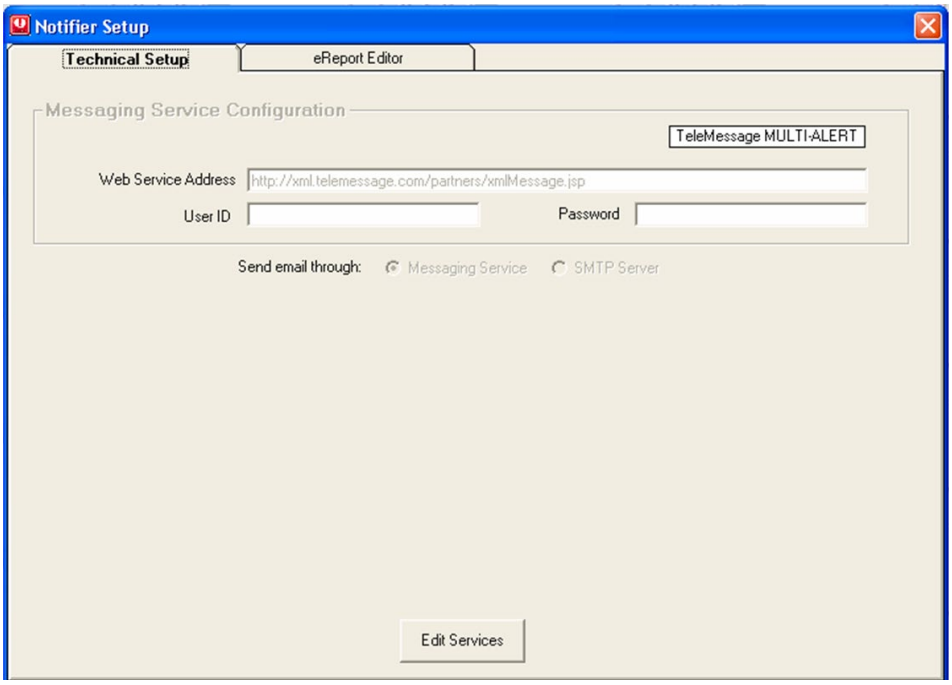


NOTIFIER

Note: This Notifier applies ONLY to NTC systems. See pages 43-53 for VTC Notifier.

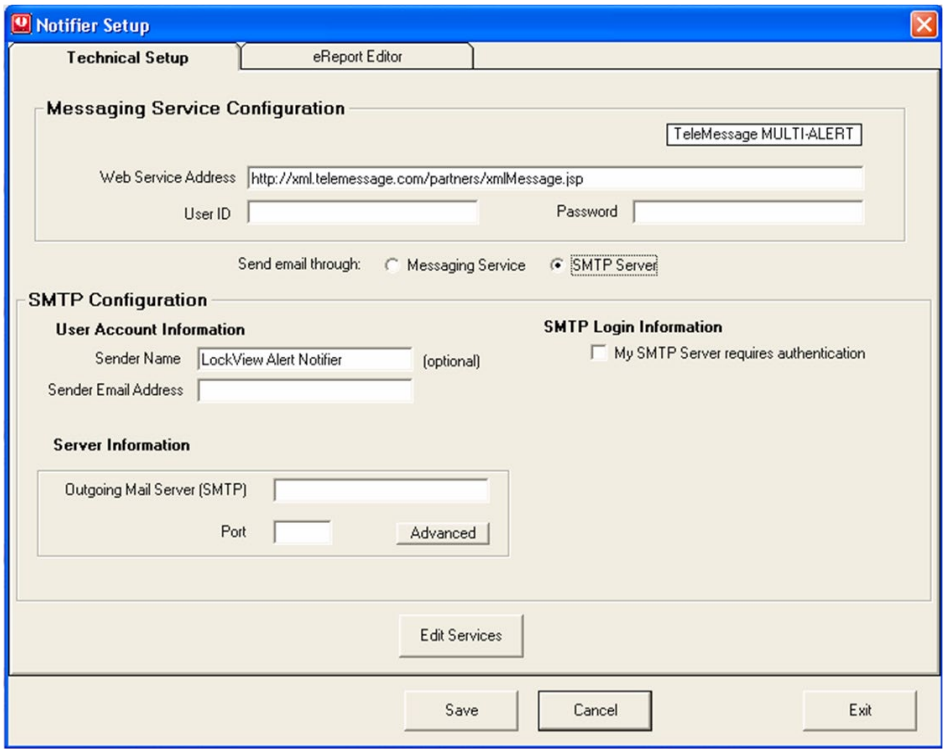
Notifier allows the LockView Operator to set up eReports. eReports can create and send (through email) audit trail reports from eLocks to a list of recipients on a programmable interval. eReports can also save these reports to a local hard drive.

The "Notifier" requires an internet connected network as well as a MSSQL database. There are two tabs in the **Notifier** menu: **Technical Setup** and **eReports Editor**.



TECHNICAL SETUP

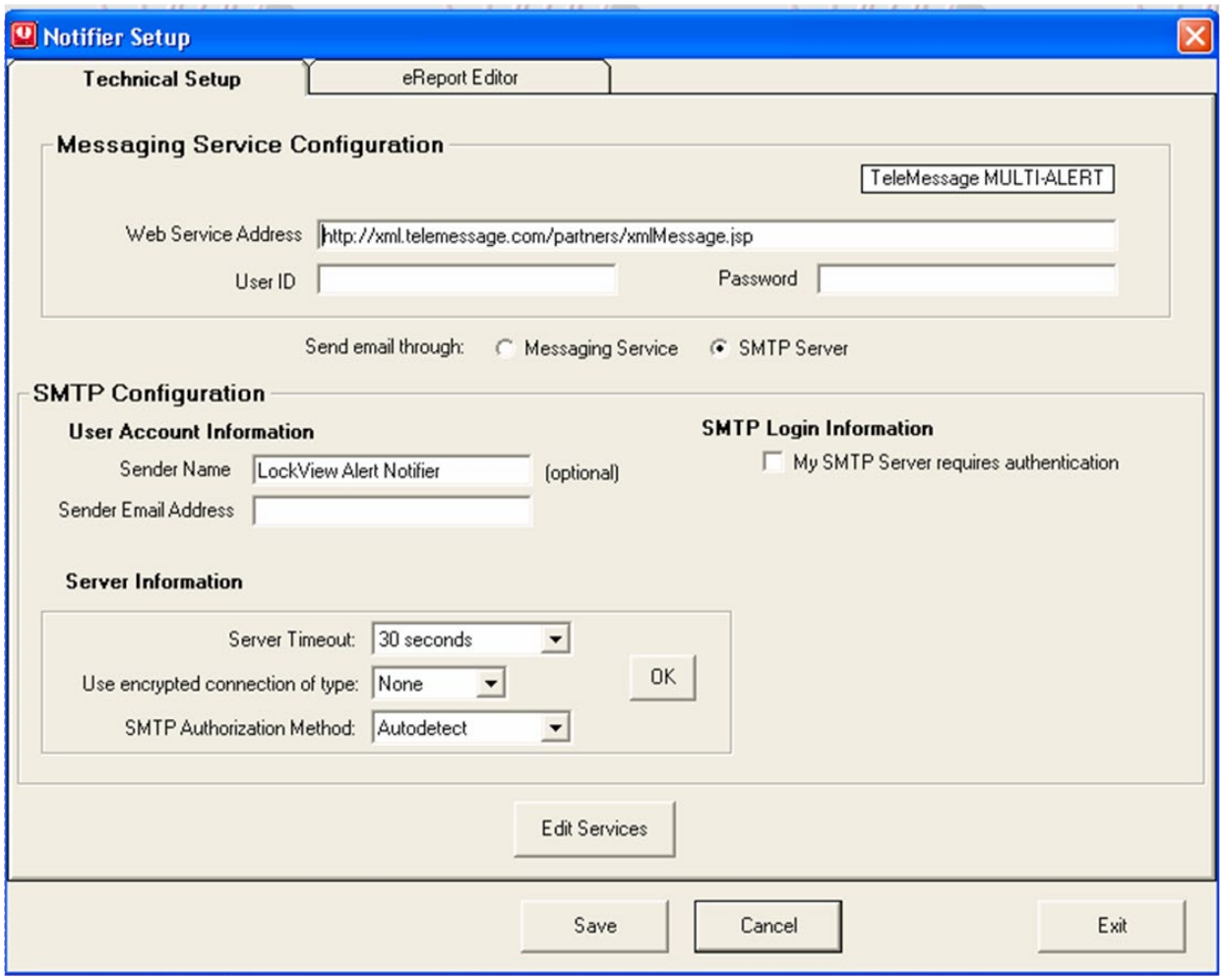
The Notifier sends alerts through SMTP or through the third party SMS provider TeleMessage. Setting up SMTP and TeleMessage is done in **Technical Setup**.



NOTIFIER continued

Note: This Notifier applies ONLY to NTC systems. See pages 43-53 for VTC Notifier.

1. To set up the SMS system, it is first required that a TeleMessage account is set up. Visit www.telemessge.com for details. A User ID and Password is required.
2. In the **Messaging Service Configuration** portion of the **Technical Setup** tab, enter the TeleMessage User ID and Password. The Web Service Address is already filled in, but can be edited if necessary.
3. Choose how an eReport will be sent; either by the messaging service (TeleMessage) or through SMTP by clicking the proper button in the middle of the **Technical Setup** window, adjacent to **Send email through**:
4. If SMTP is selected, enter the **Sender Name** and **Sender Email Address** in the **User Account Information** Section. Enter the **Outgoing Mail Server** and **Port information** in the **Server Information** area.
5. Selecting **Advanced** will open up the following options:



The additional information will allow **Server Timeout**, **Encrypted Connection** (SSL or TLS), and **SMTP Authorization Method** (auto detect, PAIN, LOGIN, or CAM-MD5) to be entered.

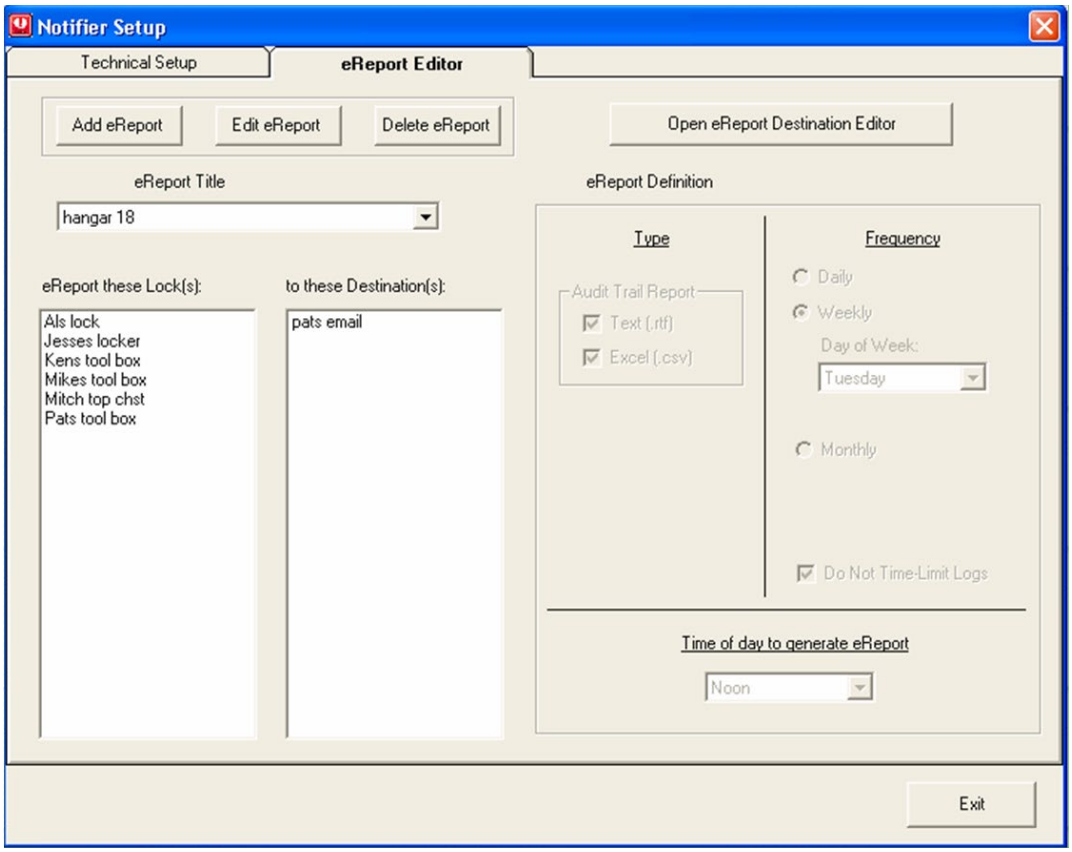
6. If the SMTP server requires authentication, user name and password can be entered in the bottom right corner of the Technical Setup tab, by clicking the box next to **My SMTP Server requires authentication**.

NOTIFIER continued

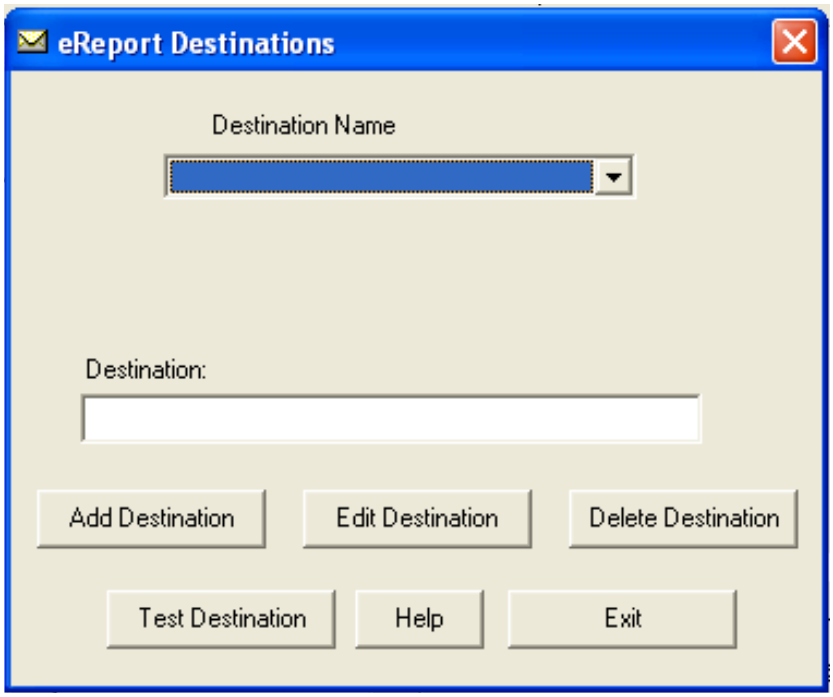
Note: This Notifier applies ONLY to NTC systems. See pages 43-53 for VTC Notifier.

eREPORTS

eReports can automatically create and send access audit trail reports from eLocks to a list of recipient's email addresses known as **Destinations** on a programmable interval. These reports can also be saved to a local hard drive.
Click the **eReports** tab of the **Notifier** to set up **eReports**



To Add/Edit/Delete **Destinations**, click the **Open eReport Destination Editor** button



NOTIFIER continued

Note: This Notifier applies ONLY to NTC systems. See pages 43-53 for VTC Notifier.

ADD DESTINATION

1. Click the **Add Destination** button in the **eReport Destinations** window of the eReport editor tab.
2. Enter the **Destination Name** and type of destination (email address or network folder)
3. If the type of destination is an email address, enter the email address.
4. If the type of destination is an network folder, click the more information button (...) and navigate to the desired network folder.
5. Click **Save**
6. Click **Exit**

EDIT DESTINATION

1. Choose the Destination be edited in the **Destination Name** pull down menu of the **eReport Destinations Editor**.
2. Click the **Edit Destination** button
3. Edit the type of destination (email address or network folder) and the details regarding the destination.
4. Click **Save**
5. Click **Exit**

DELETE DESTINATION

1. Choose the Destination to be deleted in the **Destination Name** pull down menu of the **eReport Destinations Editor**.
2. Click the **Delete Destination** button
3. Verify the deletion by clicking **OK**
4. Click **Exit**

Once destinations have been created, eReports can be created.

ADD eREPORT

1. Click the **Add eReport** button in the **eReport Editor**.
2. Enter a title for the eReport in the eReport Title entry box.
3. Choose which eLock(s) to report in the **eReport these Lock(s)** selection box.
4. Choose which destination(s) will receive the eReports in the **to these Destination(s)**: selection box.

NOTE: Multiple eReports can be sent to multiple destinations by holding Ctrl on the keyboard while clicking the destination and/or name.

5. Choose the type of report in the **eReport Definition** section. There are two formats (Text and Excel)
6. Choose how often the report will be sent in the **eReport Definition** section. There are three options available: **Daily**, **Weekly** and **Monthly**. If **Weekly** is chosen, the day of the week must be selected. If **Monthly** is chosen, the day of the month must be selected.
7. Selecting **Do Not Time-Limit Logs** will cause a full report to be sent each time. That is, all data available for that eLock will be sent every time a report is generated. If **Do Not Time-Limit Logs** is not chosen, only data accumulated since the last report was created will be sent. For example, if **Daily** is chosen, only the past day's events will be in the report.
8. Choose the time of day the report will be created and sent under **Time of day to generate eReport**.
9. Click **Save** when complete.

EDIT AN eREPORT

1. Choose the eReport to be edited in the **eReport Title** drop down menu of the **eReport Editor**.
2. Click the **Edit eReport** button.
3. Edit the desired eLock, destination, eReport type and frequency
4. Click **Save** when complete.

NOTIFIER continued

Note: This Notifier applies ONLY to NTC systems. See pages 43-53 for VTC Notifier.

DELETE AN eREPORT

1. Choose the eReport to be deleted in the **eReport Title** drop down menu of the **eReport Editor**.
2. Click the **Delete eReport** button.
3. Verify the deletion by clicking **OK**

NOTIFIER

Note: This Notifier applies ONLY to VTC systems. See pages 38-42 for NTC systems.

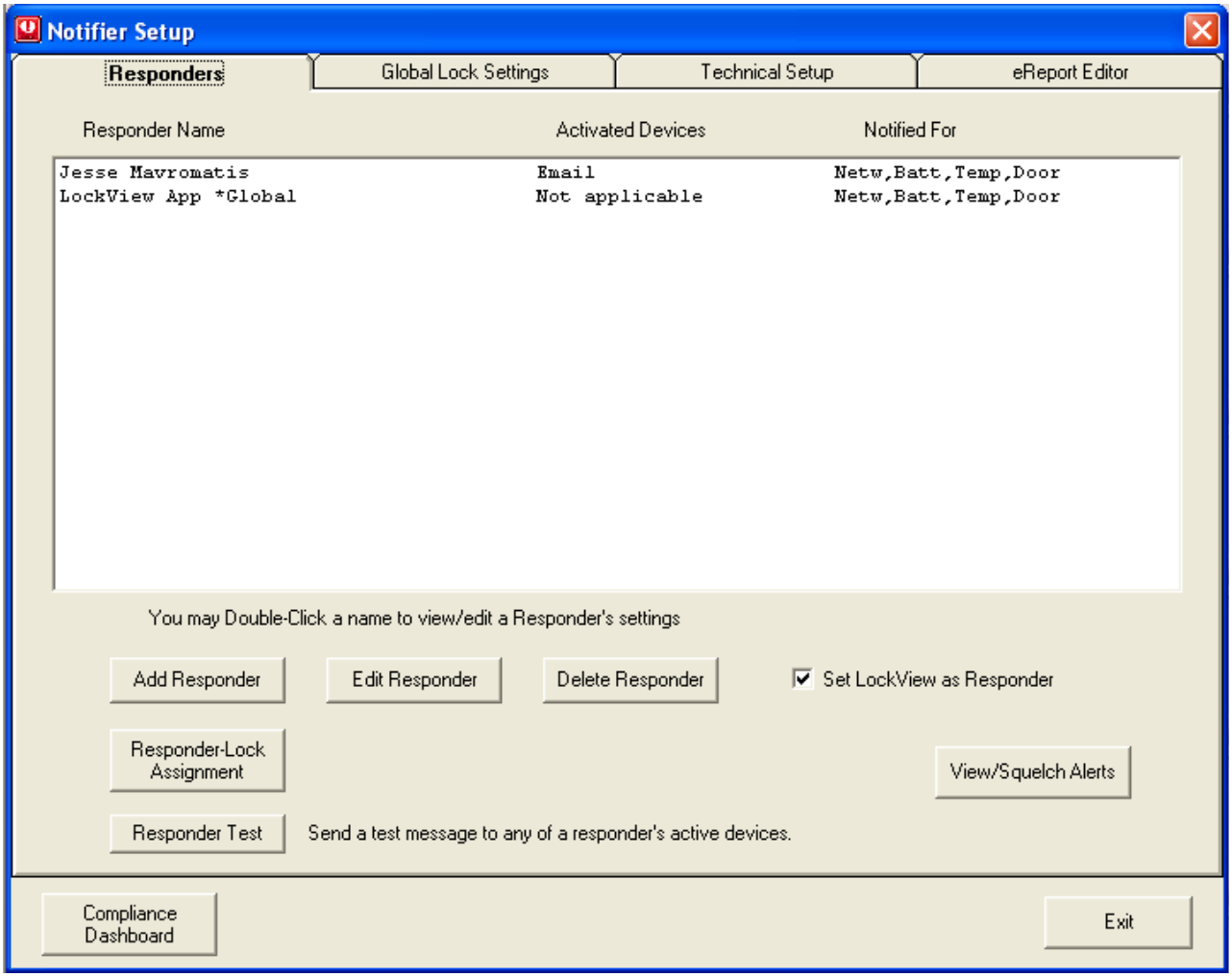
Notifier allows the LockView Operator to set up 3 different systems of notifications; Remote Notification, eReports and Compliance Dashboard. Remote Notification can be configured to send emails, text messages, phone calls, and/or faxes to a list of responders if an eLock(s) has entered a distressed mode. These modes include **Overdue Network Check-in**, **Battery Low**, **Temperature Outside Limits** and **Door Switch Alert(s)**. eReports can create and send (through email) audit trail and temperature data reports from eLocks to a list of recipients on a programmable interval. eReports can also save these reports to a local hard drive. Compliance Dashboard allows the Operator to quickly see the status of each eLock on their system in one simple window.

The "Notifier" requires an internet connected network as well as a MSSQL database.
There are four tabs in the **Notifier** menu: **Responders, Global Lock Settings, Technical Setup** and **eReports Editor**.

There are three levels of responders; 1st Responder(s), 2nd Responder(s) and 3rd Responder(s). The LockView Operator can setup a system whereby if a distressed condition(s) at the eLock(s) persists, the level of responder will escalate, from 1st Responder(s) to 2nd Responder(s) and 3rd Responder(s).

Select **Set LockView as Responder** to allow the Notifier to create and send "pop up" alert(s) that will appear on a computer that has LockView running.

The remote notification can be an email sent through SMTP, or an SMS sent via TeleMessage. TeleMessage provides text messages, fax, voice message and email. The services TeleMessage provides are not included. See **http://www.telemessage.com/download/signUpForm.jsp?loc=enUS&prodid=34** for details.

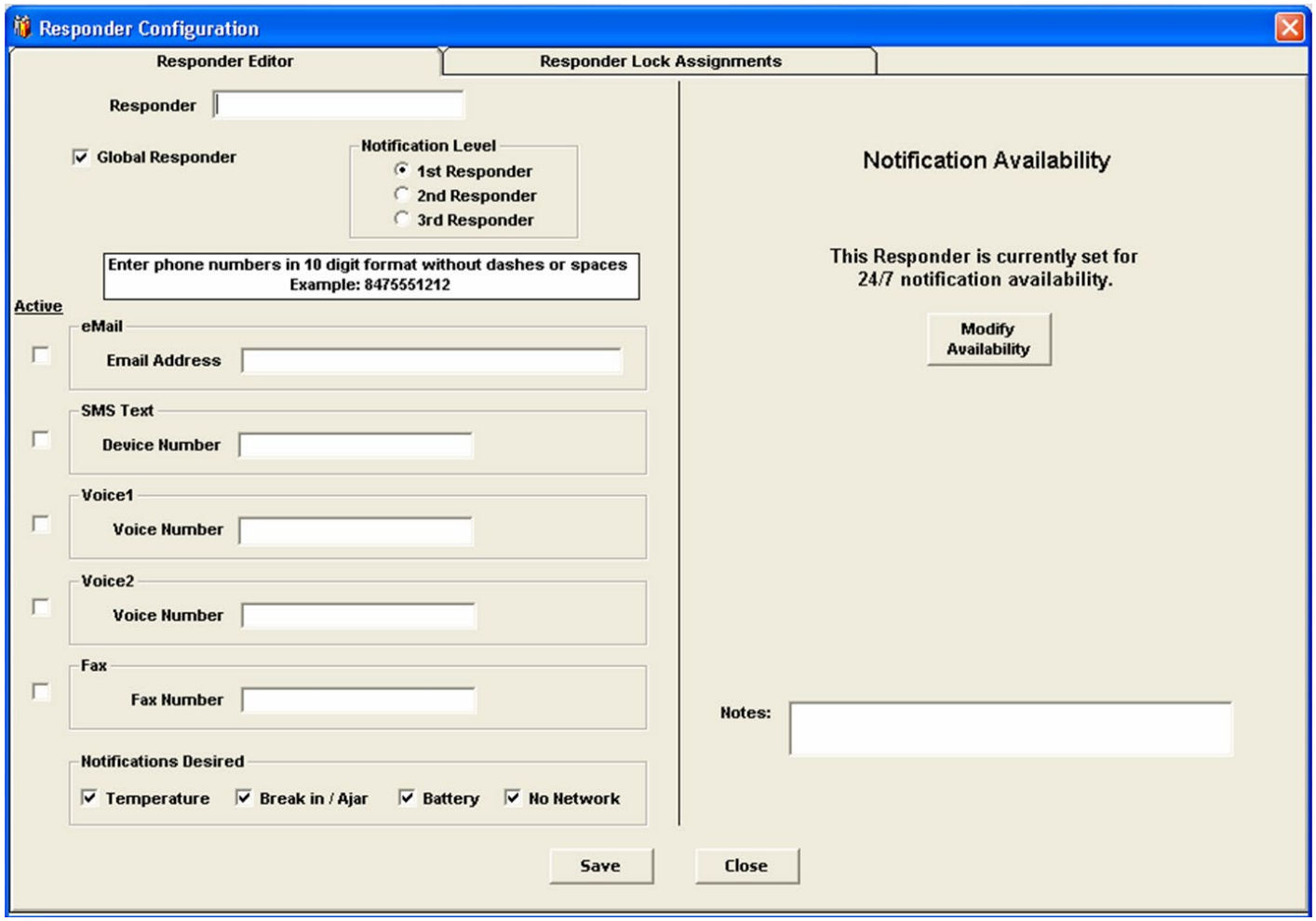


NOTIFIER continued

Note: This Notifier applies ONLY to VTC systems. See pages 38-42 for NTC systems.

ADD A RESPONDER

1. Click the **Add Responder** button in the **Responders** tab of the **Notifier** icon.
2. Enter the Responder's name in the **Responder** field.
3. Select **Global Responder** if the Responder should be notified for ALL eLocks that may enter a distressed condition.
4. Select the **Notification Level**. If an eLock enters a distressed condition, 1st Responder(s) are notified first, followed by 2nd Responder(s) and lastly 3rd Responder(s). The escalation of notification to Responders is programmable as noted on page XX.
5. Choose which method(s) of alert(s) the Responder will receive by clicking the **Active** button next to each method of notification. If an alert method is active, the destination of that notification must be entered. For example, email notification requires an email address; a text message requires a phone number equipped to receive text messages.
6. Choose which type(s) of notification(s) the Responder will receive by selecting the Notifications desired. (Temperature, Break-in, Ajar, Battery, and/or No Network)
7. If the Responder will not be available 24 hours a day/7 day a week, choose the availability by clicking **Modify Availability**. Choose the days of the week and the time of day that the responder will be available to receive messages regarding distressed eLocks.
8. Additional information regarding the Responder can be entered in the **Notes** field.
9. Click **Save** when done.



NOTIFIER continued

Note: This Notifier applies ONLY to VTC systems. See pages 38-42 for NTC systems.

EDIT A RESPONDER

1. In the **Responders** tab, highlight the responder to be edited.
2. Click the **Edit Responder** button.
3. Edit the desired fields.
4. Click **Save** to save the changes

DELETE A RESPONDER

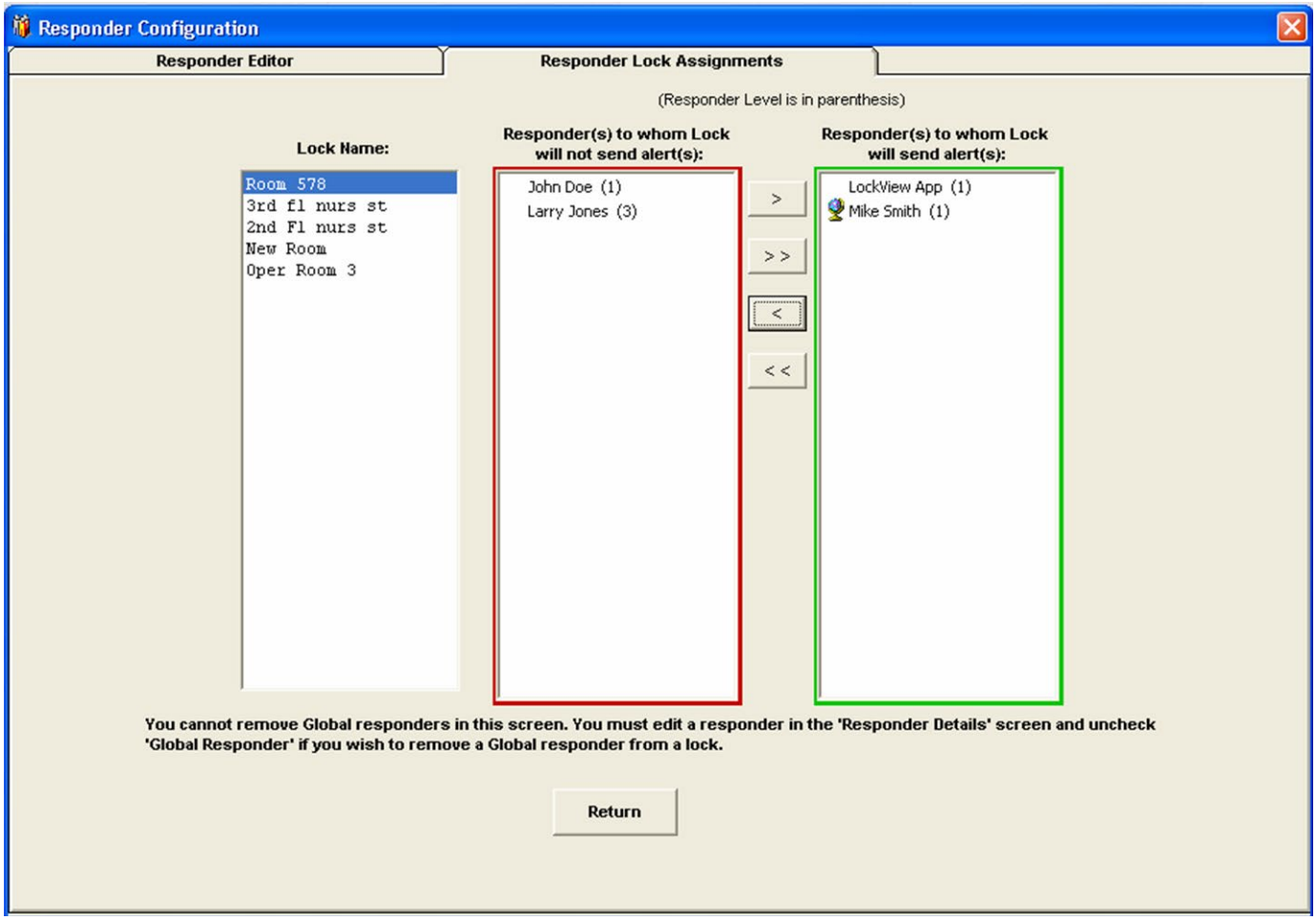
1. In the **Responders** tab, highlight the Responder to be deleted.
2. Click the **Delete Responder** button.
3. Verify then click **OK**

TEST IF A RESPONDER IS PROPERLY SET UP

1. In the **Responders** tab, highlight the Responder that is going to be tested.
2. Clicking **Responder Test** will send a test message to all of the Responder's active devices.

ASSIGN LOCKS TO RESPONDERS

Unless a Responder is global, the distressed eLock(s) to which a Responder will be notified must be selected. To assign eLock(s) to Responders, click **Responder Lock Assignments**.


Responder Configuration
Responder Editor
Responder Lock Assignments
(Responder Level is in parenthesis)
Lock Name:
Responder(s) to whom Lock will not send alert(s):
Responder(s) to whom Lock will send alert(s):
Room 578
3rd fl nurs st
2nd Fl nurs st
New Room
Oper Room 3
John Doe (1)
Larry Jones (3)
LockView App (1)
Mike Smith (1)
>
>>
<
<<
You cannot remove Global responders in this screen. You must edit a responder in the 'Responder Details' screen and uncheck 'Global Responder' if you wish to remove a Global responder from a lock.
Return

NOTIFIER continued

Note: This Notifier applies ONLY to VTC systems. See pages 38-42 for NTC systems.

1. Choose the eLock to which the Responder(s) is/are assigned by highlighting the **Lock Name**. This will bring up the list of Responders in the next two columns.
   - The Responder(s) in the red box are **Responder(s) to whom the lock will not send alert(s)**.
   - The Responder(s) in the green box are **Responder(s) to whom the lock will send alert(s)**.
   - If Show Instant Notifications is selected, a pop-up will appear on the computer screen. If/when an eLock(s) goes into an alarming mode (LockView program must be running in order to see the pop-up alert)

   NOTE*: The number in the parenthesis following the Responder name corresponds to their notification level.*

   - A globe icon next to the Responder name identifies that they are a Global Responder.

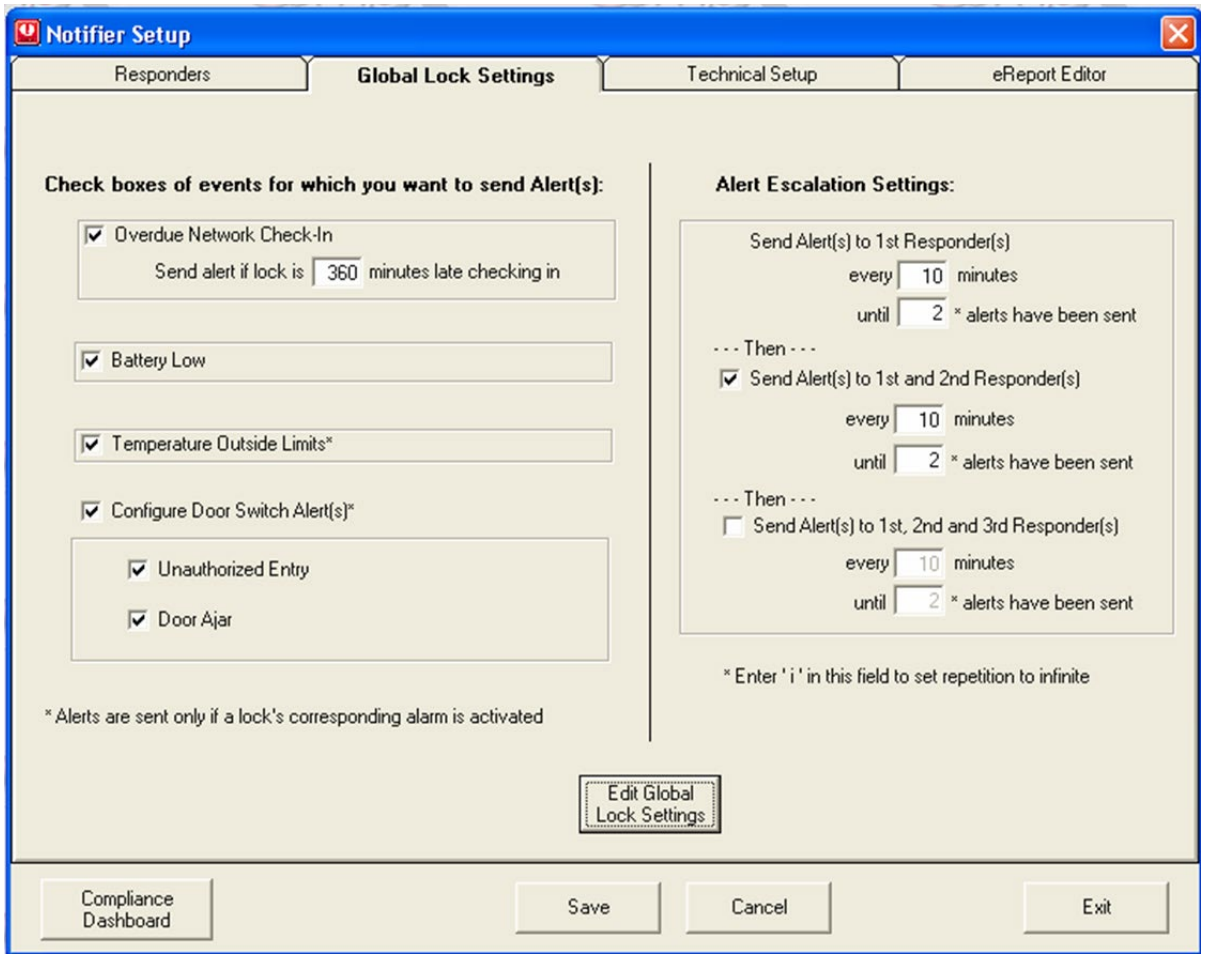
2. To change which Responders will be notified, select the Responder and click the appropriate single arrow; moving the Responder from the red box to the green, or vice versa. **NOTE**: Global Responders reside in the green box and cannot be moved to the red box.

3. To change ALL Responders status for the eLock, click the appropriate double arrow; moving ALL Responders from the red box to the green, or vice versa.

GLOBAL LOCK SETTINGS

All eLocks in the Notifier system will have global settings or individual settings. Global settings allow the LockView Operator to manage multiple similar eLocks simultaneously; without having to adjust each one individually.

Click the **Global Lock Settings** tab to adjust the global lock settings.


Notifier Setup
Responders
Global Lock Settings
Technical Setup
eReport Editor
Check boxes of events for which you want to send Alert(s):
Overdue Network Check-In
Send alert if lock is 360 minutes late checking in
Battery Low
Temperature Outside Limits*
Configure Door Switch Alert(s)*
Unauthorized Entry
Door Ajar
* Alerts are sent only if a lock's corresponding alarm is activated
Alert Escalation Settings:
Send Alert(s) to 1st Responder(s)
every 10 minutes
until 2 * alerts have been sent
- - - Then - - -
Send Alert(s) to 1st and 2nd Responder(s)
every 10 minutes
until 2 * alerts have been sent
- - - Then - - -
Send Alert(s) to 1st, 2nd and 3rd Responder(s)
every 10 minutes
until 2 * alerts have been sent
* Enter ' i ' in this field to set repetition to infinite
Edit Global Lock Settings
Compliance Dashboard
Save
Cancel
Exit

NOTIFIER continued

Note: This Notifier applies ONLY to VTC systems. See pages 38-42 for NTC systems.

PROGRAMMING GLOBAL LOCK SETTINGS

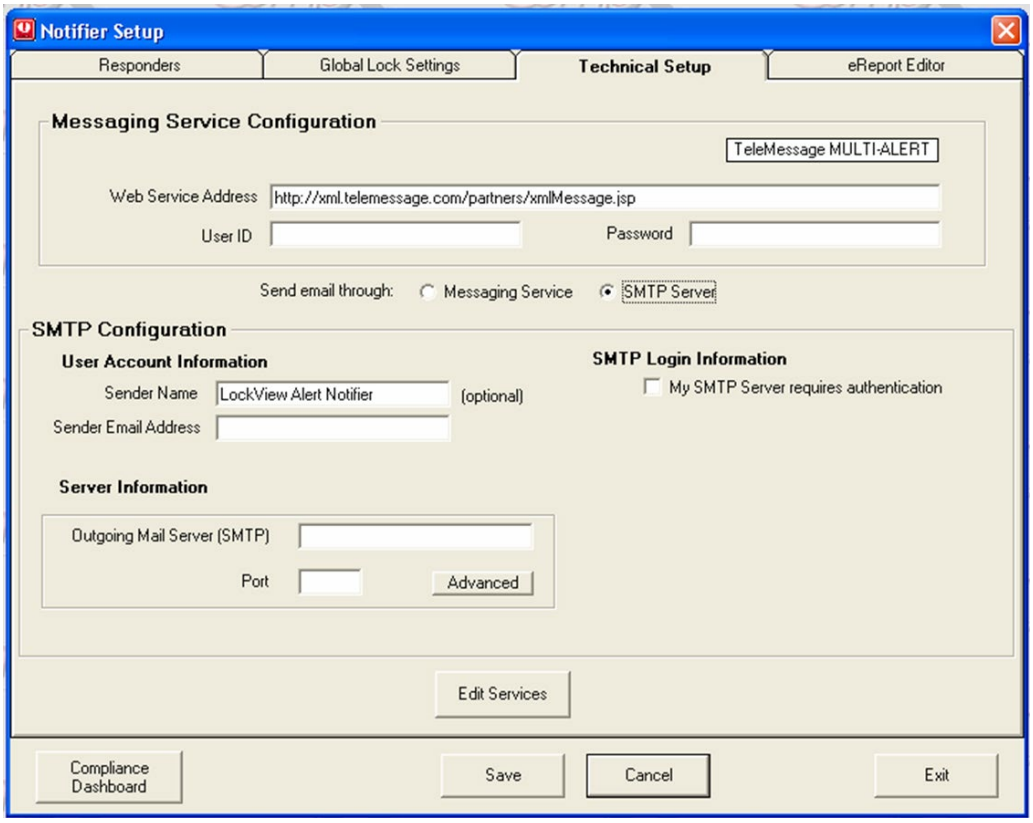
1. Clock **Edit Global Lock Settings** box.
2. Choose the eLock distress events for which notification is globally desired.
   - Selecting **Overdue Network Check-In** will send a notification if an eLock has missed the programmed scheduled network update (see **Lock Editor-Networked eLock Scheduler** on page 22).
   - Selecting **Battery Low** will send a notification if the battery power drops to "LOW."
   - Selecting **Temperature Outside Limits/Probe Failure** will send a notification if the eLock has 1) temperature alarming enabled, 2) the current temperature is outside of the high/low limits and 3) the temperature has been outside of the specified limits for a time exceeding the **Alarm Delay**.
     NOTE: This notification only applies to eLocks equipped with temperature monitoring.
   - Notification can be sent for the two types of **Door Switch Alerts**. Selecting **Unauthorized Entry** will send notification if the door switch opens at any time not immediately following the presentation of a valid credential. Selecting **Door Ajar** will send notification if the door has been open for a programmable amount of time past the standard eLock open time (see **Lock Editor-Door Switch Menu** on page 22). **NOTE**: This notification only applies to eLocks with door switch hardware.
3. **Alert Escalation Settings** allows the LockView Operator to set up a schedule for how often and how many alert(s) will be sent to the Responder(s).
   - Enter how often and how many alert(s) will be sent to the 1st Responder(s) before escalating to the 2nd Responder(s).
   - Enter how often and how many alert(s) will be sent to the 2nd Responder(s) before escalating to the 3rd Responder(s).
   - Enter how often and how many alert(s) will be sent to the 3rd Responder(s)

   NOTE: *Entering an "i" in the number of alerts field will force an infinite number of alerts.*

4. Click **Save** when done.

TECHNICAL SETUP

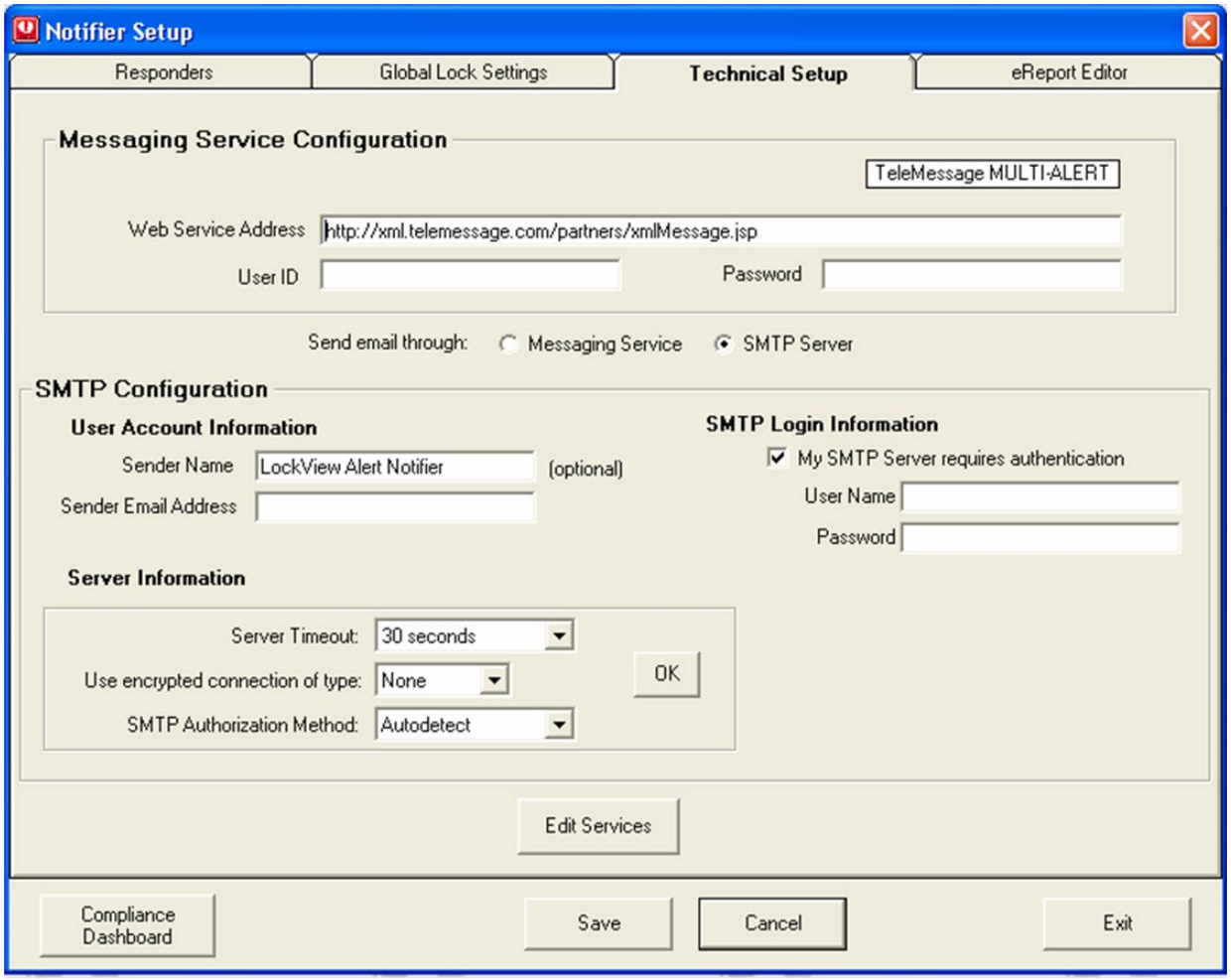
The Notifier sends alerts through SMTP or through the third party SMS provider TeleMessage. Setting up SMTP and TeleMessage is done in **Technical Setup**.



NOTIFIER continued

Note: This Notifier applies ONLY to VTC systems. See pages 38-42 for NTC systems.

1. To set up the SMS system, it is first required that a TeleMessage account is set up. Visit www.telemessge.com for details. A User ID and Password is required.
2. In the **Messaging Service Configuration** portion of the **Technical Setup** tab, enter the TeleMessage User ID and Password. The Web Service Address is already filled in, but can be edited if necessary.
3. Choose how an email notification will be sent; either by the messaging service (TeleMessage) or through SMTP by clicking the proper button in the middle of the **Technical Setup** window, adjacent to **Send email through**:
4. If SMTP is selected, enter the **Sender Name** and **Sender Email Address** in the **User Account Information** Section. Enter the **Outgoing Mail Server** and **Port information** in the **Server Information** area.
5. Selecting **Advanced** will open up the following options:



The additional information will allow **Server Timeout**, **Encrypted Connection** (SSL or TLS), and **SMTP Authorization Method** (auto detect, PAIN, LOGIN, or CAM-MD5) to be entered.

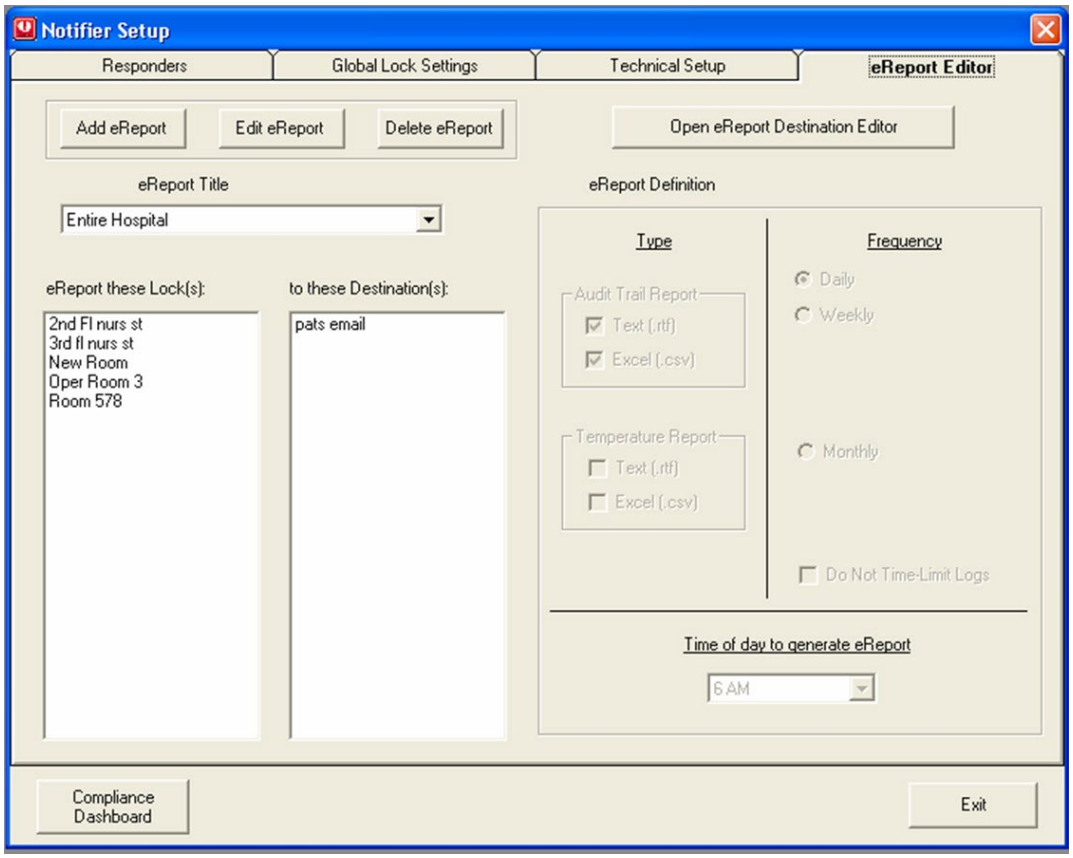
6. If the SMTP server requires authentication, user name and password can be entered in the bottom right corner of the Technical Setup tab, by clicking the box next to **My SMTP Server requires authentication**.

NOTIFIER continued

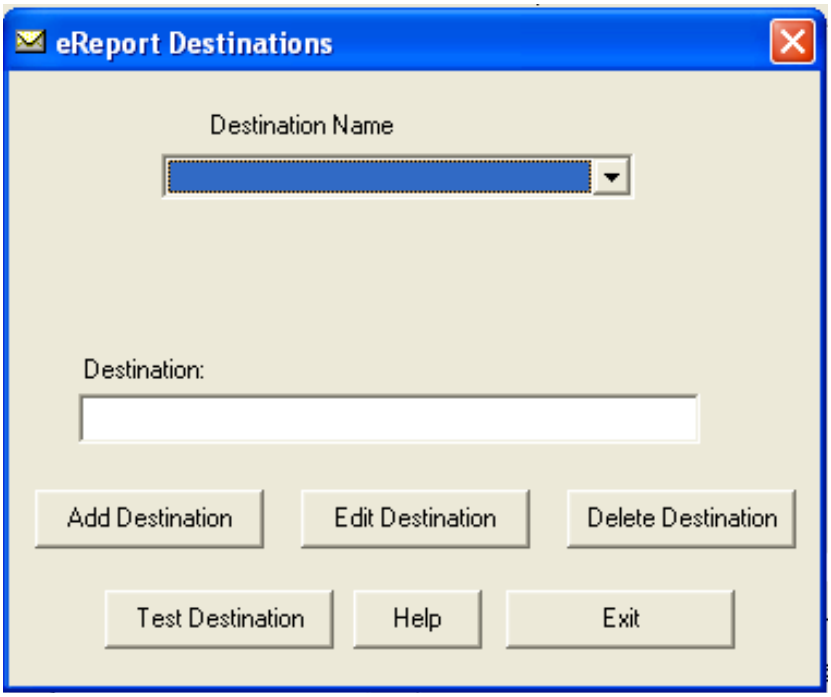
Note: This Notifier applies ONLY to VTC systems. See pages 38-42 for NTC systems.

eREPORTS

eReports can automatically create and send access audit trail and temperature data reports from eLocks to a list of recipient's email addresses known as **Destinations** on a programmable interval. These reports can also be saved to a local hard drive. Click the **eReports** tab of the **Notifier** to set up **eReports**



To Add/Edit/Delete **Destinations**, click the **Open eReport Destination Editor** button



NOTIFIER continued

Note: This Notifier applies ONLY to VTC systems. See pages 38-42 for NTC systems.

ADD DESTINATION

1. Click the **Add Destination** button in the **eReport Destinations** window of the eReport editor tab.
2. Enter the **Destination Name** and type of destination (email address or network folder)
3. If the type of destination is an email address, enter the email address.
4. If the type of destination is an network folder, click the more information button (...) and navigate to the desired network folder.
5. Click **Save**
6. Click **Exit**

EDIT DESTINATION

1. Choose the Destination be edited in the **Destination Name** pull down menu of the **eReport Destinations Editor**.
2. Click the **Edit Destination** button
3. Edit the type of destination (email address or network folder) and the details regarding the destination.
4. Click **Save**
5. Click **Exit**

DELETE DESTINATION

1. Choose the Destination to be deleted in the **Destination Name** pull down menu of the **eReport Destinations Editor**.
2. Click the **Delete Destination** button
3. Verify the deletion by clicking **OK**
4. Click **Exit**

Once destinations have been created, eReports can be created.

ADD eREPORT

1. Click the **Add eReport** button in the **eReport Editor**.
2. Enter a title for the eReport in the eReport Title entry box.
3. Choose which eLock(s) to report in the **eReport these Lock(s)** selection box.
4. Choose which destination(s) will receive the eReports in the **to these Destination(s)**: selection box.

NOTE: Multiple eReports can be sent to multiple destinations by holding Ctrl on the keyboard while clicking the destination and/or name.

5. Choose the type of report in the **eReport Definition** section. There are two report types (access audit trail and temperature) and two formats (Text and Excel)
6. Choose how often the report will be sent in the **eReport Definition** section. There are three options available: **Daily**, **Weekly** and **Monthly**. If **Weekly** is chosen, the day of the week must be selected. If **Monthly** is chosen, the day of the month must be selected.
7. Selecting **Do Not Time-Limit Logs** will cause a full report to be sent each time. That is, all data available for that eLock will be sent every time a report is generated. If **Do Not Time-Limit Logs** is not chosen, only data accumulated since the last report was created will be sent. For example, if **Daily** is chosen, only the past day's events will be in the report.
8. Choose the time of day the report will be created and sent under **Time of day to generate eReport**.
9. Click **Save** when complete.

EDIT AN eREPORT

1. Choose the eReport to be edited in the **eReport Title** drop down menu of the **eReport Editor**.
2. Click the **Edit eReport** button.
3. Edit the desired eLock, destination, eReport type and frequency
4. Click **Save** when complete.

NOTIFIER continued

Note: This Notifier applies ONLY to VTC systems. See pages 38-42 for NTC systems.

DELETE AN eREPORT

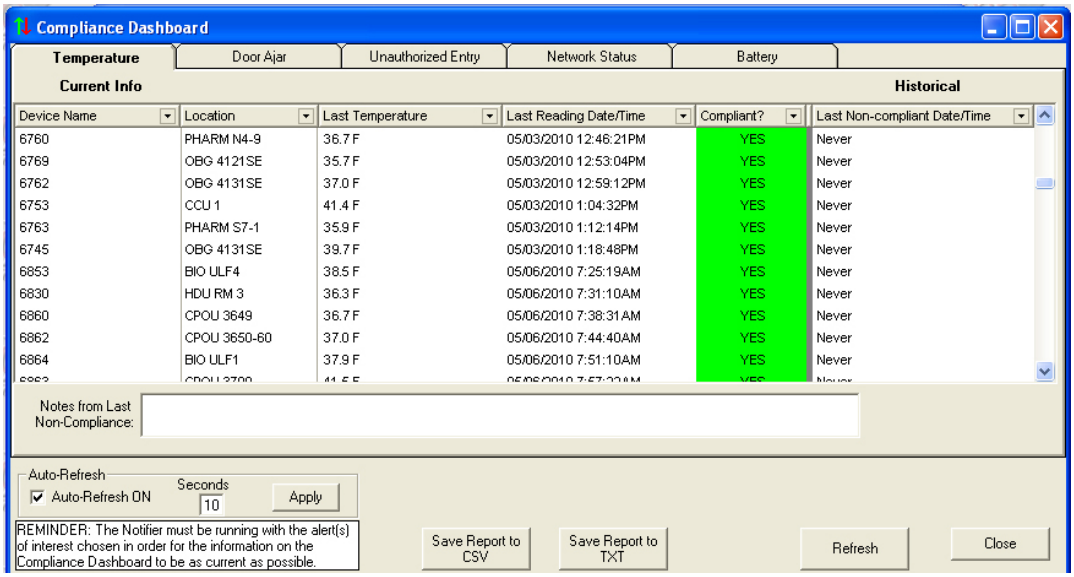
1. Choose the eReport to be deleted in the **eReport Title** drop down menu of the **eReport Editor**.
2. Click the **Delete eReport** button.
3. Verify the deletion by clicking **OK**

COMPLIANCE DASHBOARD

At the bottom of the **Notifer** is the **Compliance Dashboard** button. The **Compliance Dashboard** provides the Operator a current and historical quick look at Temperature (if equipped) door position: Ajar & Unauthorized Entry (if equipped), Network Status (if equipped), and Battery Level of all eLocks in the database.

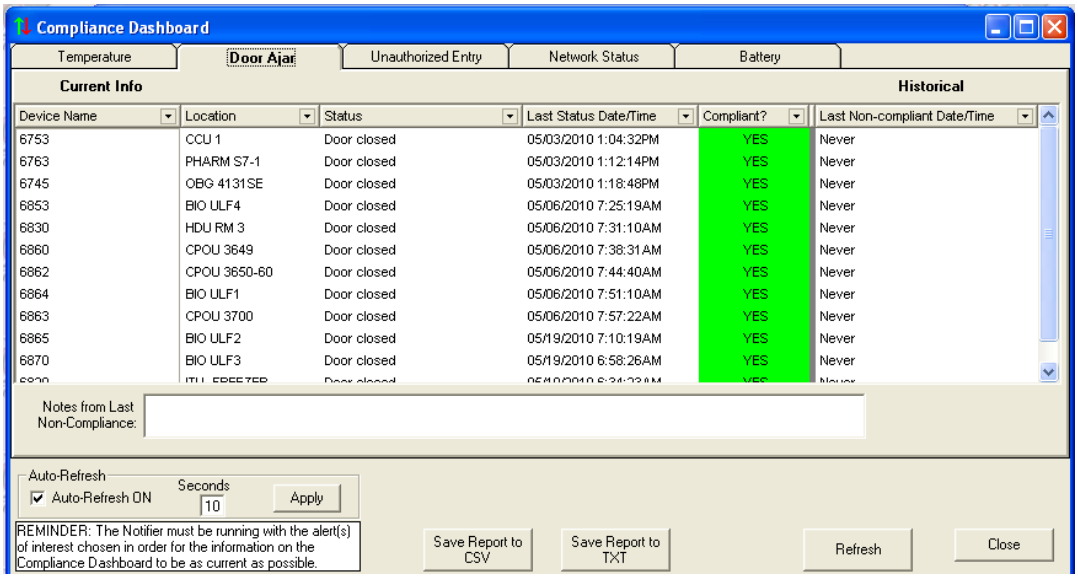
TEMPERATURE DASHBOARD (NOTE: VTC SYSTEMS DO NOT HAVE TEMPERATURE MONITORING)

Select the **Temperature** tab to view the Location, Last Temperature, Last Reading Date/Time, Compliance status, and Last Non-compliant date/time for each eLock with a temperature monitoring system.


Compliance Dashboard
Temperature
Door Ajar
Unauthorized Entry
Network Status
Battery
Current Info
Historical
Device Name
Location
Last Temperature
Last Reading Date/Time
Compliant?
Last Non-compliant Date/Time
6760 PHARM N4-9 36.7 F 05/03/2010 12:46:21PM YES Never
6769 OBG 4121SE 35.7 F 05/03/2010 12:53:04PM YES Never
6762 OBG 4131SE 37.0 F 05/03/2010 12:59:12PM YES Never
6753 CCU 1 41.4 F 05/03/2010 1:04:32PM YES Never
6763 PHARM S7-1 35.9 F 05/03/2010 1:12:14PM YES Never
6745 OBG 4131SE 39.7 F 05/03/2010 1:18:48PM YES Never
6853 BIO ULF4 38.5 F 05/06/2010 7:25:19AM YES Never
6830 HDU RM 3 36.3 F 05/06/2010 7:31:10AM YES Never
6860 CPOU 3649 36.7 F 05/06/2010 7:38:31AM YES Never
6862 CPOU 3650-60 37.0 F 05/06/2010 7:44:40AM YES Never
6864 BIO ULF1 37.9 F 05/06/2010 7:51:10AM YES Never
Notes from Last Non-Compliance:
Auto-Refresh
Auto-Refresh ON
Seconds
10
Apply
REMINDER: The Notifier must be running with the alert(s) of interest chosen in order for the information on the Compliance Dashboard to be as current as possible.
Save Report to CSV
Save Report to TXT
Refresh
Close

DOOR AJAR DASHBOARD

Select the **Door Ajar** tab to view the Location, door ajar Status, Last Status Date/Time, Compliance status, and Last Non-compliant date/time for each eLock with door switch installed.

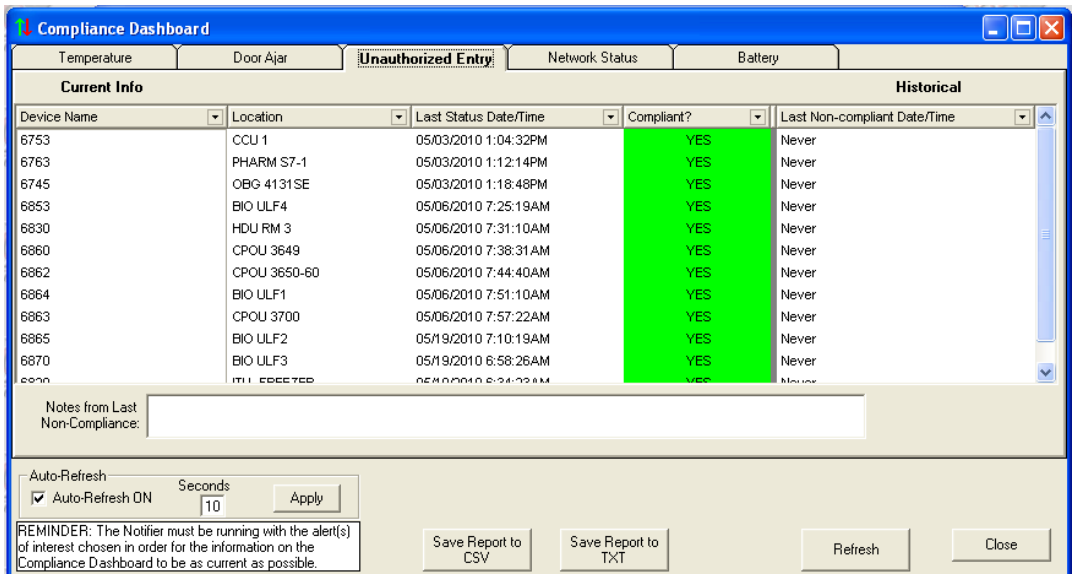

Compliance Dashboard
Temperature
Door Ajar
Unauthorized Entry
Network Status
Battery
Current Info
Historical
Device Name
Location
Status
Last Status Date/Time
Compliant?
Last Non-compliant Date/Time
6753 CCU 1 Door closed 05/03/2010 1:04:32PM YES Never
6763 PHARM S7-1 Door closed 05/03/2010 1:12:14PM YES Never
6745 OBG 4131SE Door closed 05/03/2010 1:18:48PM YES Never
6853 BIO ULF4 Door closed 05/06/2010 7:25:19AM YES Never
6830 HDU RM 3 Door closed 05/06/2010 7:31:10AM YES Never
6860 CPOU 3649 Door closed 05/06/2010 7:38:31AM YES Never
6862 CPOU 3650-60 Door closed 05/06/2010 7:44:40AM YES Never
6864 BIO ULF1 Door closed 05/06/2010 7:51:10AM YES Never
6863 CPOU 3700 Door closed 05/06/2010 7:57:22AM YES Never
6865 BIO ULF2 Door closed 05/19/2010 7:10:19AM YES Never
6870 BIO ULF3 Door closed 05/19/2010 6:58:26AM YES Never
Notes from Last Non-Compliance:
Auto-Refresh
Auto-Refresh ON
Seconds
10
Apply
REMINDER: The Notifier must be running with the alert(s) of interest chosen in order for the information on the Compliance Dashboard to be as current as possible.
Save Report to CSV
Save Report to TXT
Refresh
Close

NOTIFIER continued

Note: This Notifier applies ONLY to VTC systems. See pages 38-42 for NTC systems.

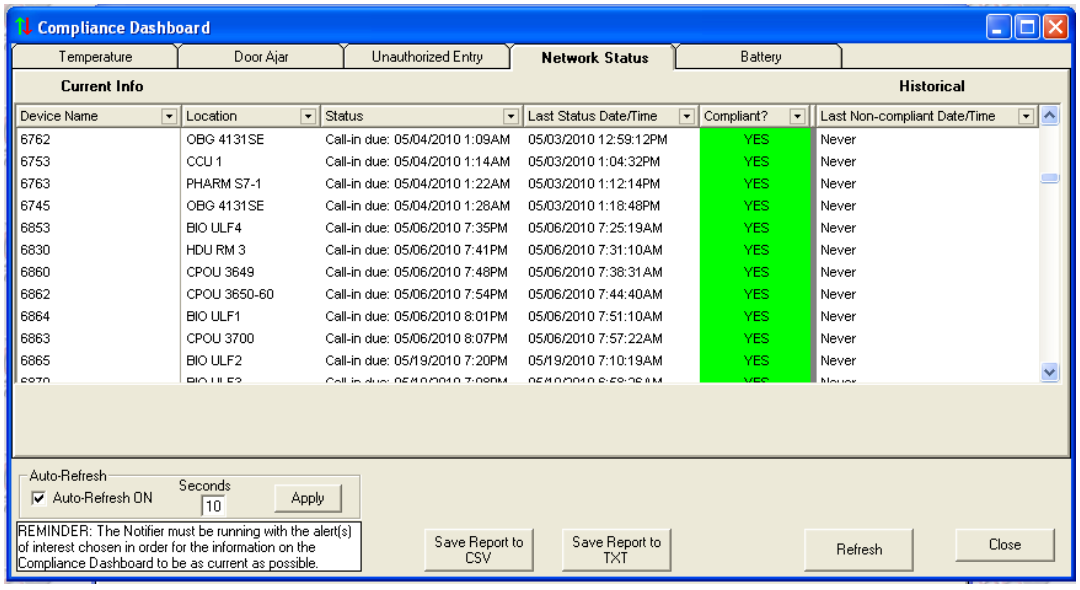
UNAUTHORIZED ENTRY DASHBOARD

Select the **Unauthorized Entry** tab to view the Location, Last Status Date/Time, Compliance status, and Last Non-compliant date/time for each eLock with door switch installed.


Compliance Dashboard
Temperature
Door Ajar
Unauthorized Entry
Network Status
Battery
Current Info
Historical
Device Name
Location
Last Status Date/Time
Compliant?
Last Non-compliant Date/Time
6753 CCU 1 05/03/2010 1:04:32PM YES Never
6763 PHARM S7-1 05/03/2010 1:12:14PM YES Never
6745 OBG 4131SE 05/03/2010 1:18:48PM YES Never
6853 BIO ULF4 05/06/2010 7:25:19AM YES Never
6830 HDU RM 3 05/06/2010 7:31:10AM YES Never
6860 CPOU 3649 05/06/2010 7:38:31AM YES Never
6862 CPOU 3650-60 05/06/2010 7:44:40AM YES Never
6864 BIO ULF1 05/06/2010 7:51:10AM YES Never
6863 CPOU 3700 05/06/2010 7:57:22AM YES Never
6865 BIO ULF2 05/19/2010 7:10:19AM YES Never
6870 BIO ULF3 05/19/2010 6:58:26AM YES Never
Notes from Last Non-Compliance:
Auto-Refresh
Auto-Refresh ON
Seconds
10
Apply
REMINDER: The Notifier must be running with the alert(s) of interest chosen in order for the information on the Compliance Dashboard to be as current as possible.
Save Report to CSV
Save Report to TXT
Refresh
Close

NETWORK STATUS DASHBOARD

Select the **Network Status** tab to view the Location, network Status, Last Status Date/Time, Compliance status, and Last Non-compliant date/time for each networked eLock on the system.

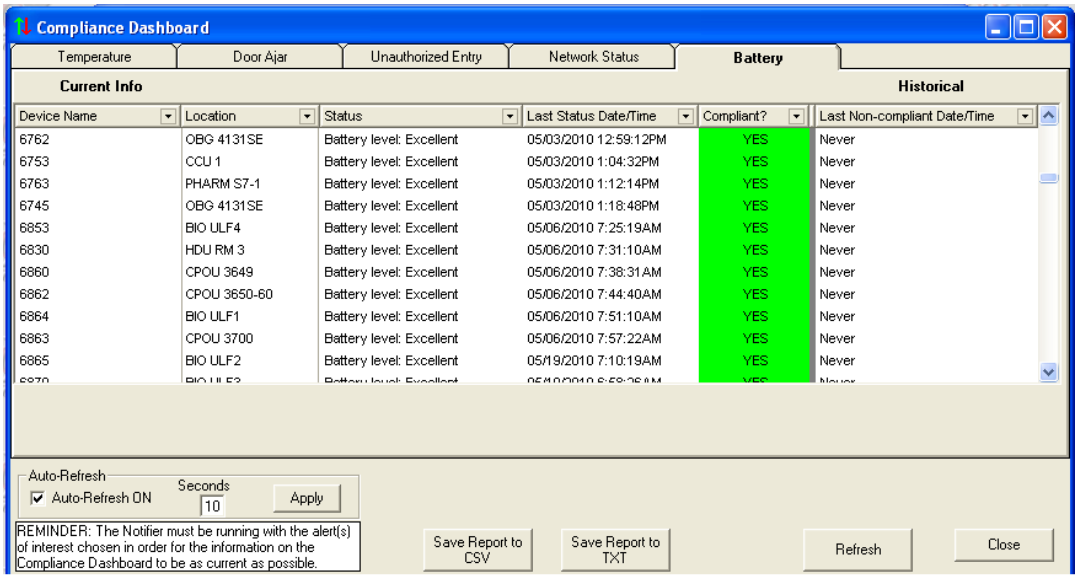

Compliance Dashboard
Temperature
Door Ajar
Unauthorized Entry
Network Status
Battery
Current Info
Historical
Device Name
Location
Status
Last Status Date/Time
Compliant?
Last Non-compliant Date/Time
6762 OBG 4131SE Call-in due: 05/04/2010 1:09AM 05/03/2010 12:59:12PM YES Never
6753 CCU 1 Call-in due: 05/04/2010 1:14AM 05/03/2010 1:04:32PM YES Never
6763 PHARM S7-1 Call-in due: 05/04/2010 1:22AM 05/03/2010 1:12:14PM YES Never
6745 OBG 4131SE Call-in due: 05/04/2010 1:28AM 05/03/2010 1:18:48PM YES Never
6853 BIO ULF4 Call-in due: 05/06/2010 7:35PM 05/06/2010 7:25:19AM YES Never
6830 HDU RM 3 Call-in due: 05/06/2010 7:41PM 05/06/2010 7:31:10AM YES Never
6860 CPOU 3649 Call-in due: 05/06/2010 7:48PM 05/06/2010 7:38:31AM YES Never
6862 CPOU 3650-60 Call-in due: 05/06/2010 7:54PM 05/06/2010 7:44:40AM YES Never
6864 BIO ULF1 Call-in due: 05/06/2010 8:01PM 05/06/2010 7:51:10AM YES Never
6863 CPOU 3700 Call-in due: 05/06/2010 8:07PM 05/06/2010 7:57:22AM YES Never
6865 BIO ULF2 Call-in due: 05/19/2010 7:20PM 05/19/2010 7:10:19AM YES Never
Auto-Refresh
Auto-Refresh ON
Seconds
10
Apply
REMINDER: The Notifier must be running with the alert(s) of interest chosen in order for the information on the Compliance Dashboard to be as current as possible.
Save Report to CSV
Save Report to TXT
Refresh
Close

NOTIFIER continued

Note: This Notifier applies ONLY to VTC systems. See pages 38-42 for NTC systems.

BATTERY DASHBOARD

Select the **Battery** tab to view the Location, battery Status, Last Status Date/Time, Compliance status, and Last Non-compliant date/time for each eLock on the system.


Compliance Dashboard
Temperature
Door Ajar
Unauthorized Entry
Network Status
Battery
Current Info
Historical
Device Name
Location
Status
Last Status Date/Time
Compliant?
Last Non-compliant Date/Time
6762 OBG 4131SE Battery level: Excellent 05/03/2010 12:59:12PM YES Never
6753 CCU 1 Battery level: Excellent 05/03/2010 1:04:32PM YES Never
6763 PHARM S7-1 Battery level: Excellent 05/03/2010 1:12:14PM YES Never
6745 OBG 4131SE Battery level: Excellent 05/03/2010 1:18:48PM YES Never
6853 BIO ULF4 Battery level: Excellent 05/06/2010 7:25:19AM YES Never
6830 HDU RM 3 Battery level: Excellent 05/06/2010 7:31:10AM YES Never
6860 CPOU 3649 Battery level: Excellent 05/06/2010 7:38:31AM YES Never
6862 CPOU 3650-60 Battery level: Excellent 05/06/2010 7:44:40AM YES Never
6864 BIO ULF1 Battery level: Excellent 05/06/2010 7:51:10AM YES Never
6863 CPOU 3700 Battery level: Excellent 05/06/2010 7:57:22AM YES Never
6865 BIO ULF2 Battery level: Excellent 05/19/2010 7:10:19AM YES Never
Auto-Refresh
Auto-Refresh ON
Seconds
10
Apply
REMINDER: The Notifier must be running with the alert(s) of interest chosen in order for the information on the Compliance Dashboard to be as current as possible.
Save Report to CSV
Save Report to TXT
Refresh
Close

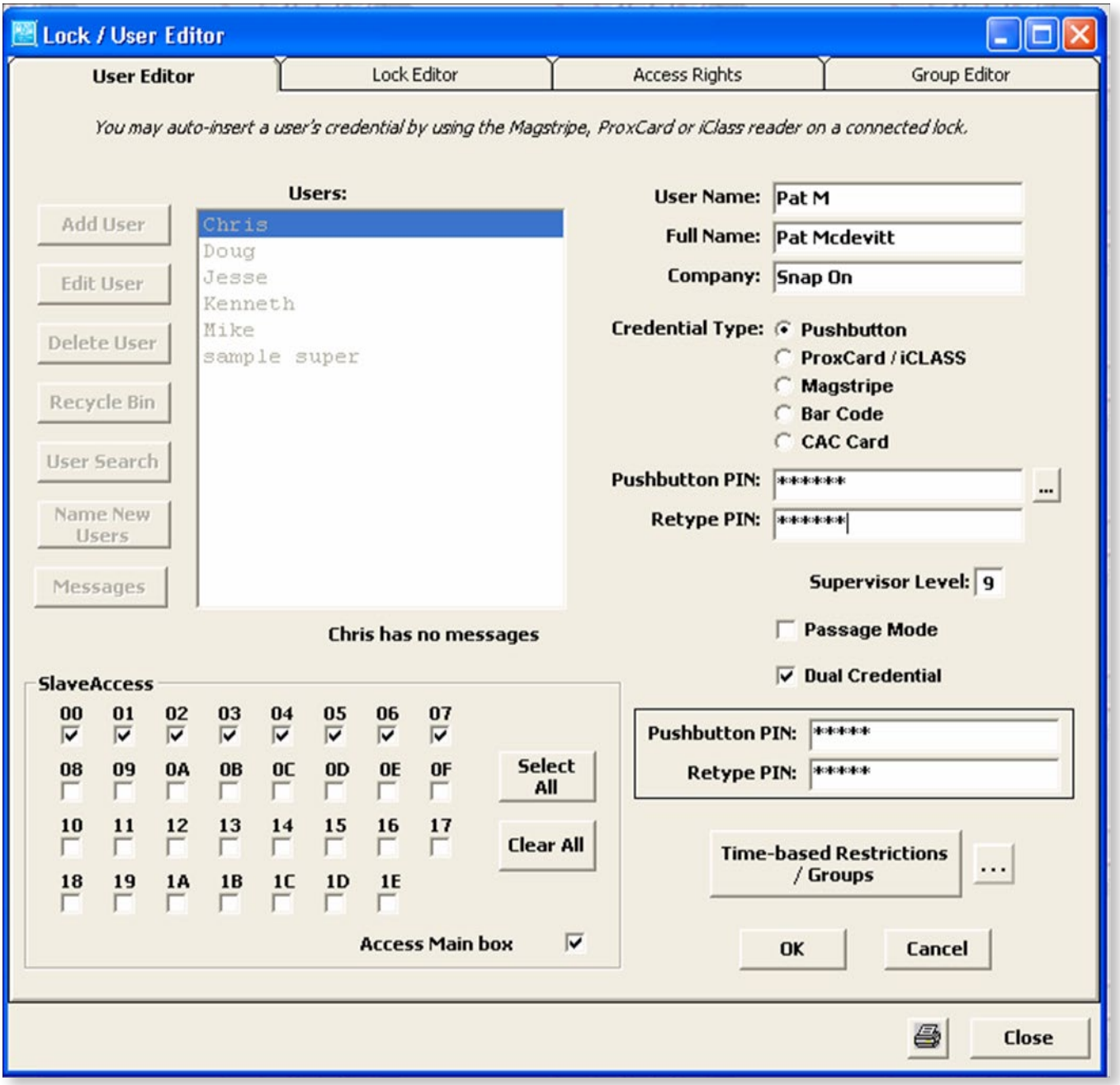
PROGRAMMING EXAMPLE

Follow this example as two new users are added into the computer database and then added into a lock's database.

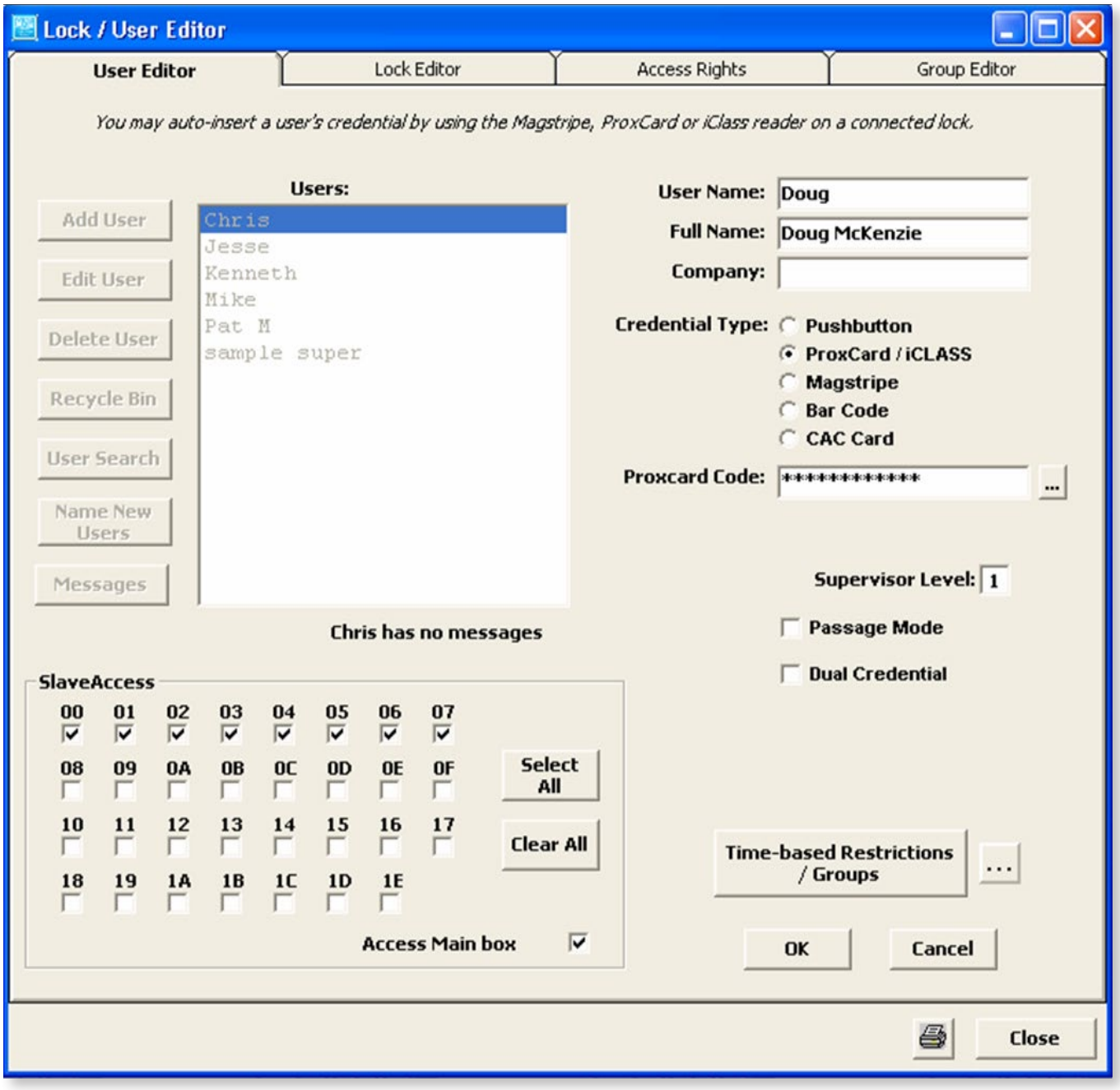
1. Select **Lock/User Editor**.
2. Select **Add User** and enter new user's information.

See pages 9-14 for more information on what each entry in the **User Editor** means.

NOTE: *The following screens show a new user being added to the computer database.*



PROGRAMMING EXAMPLE continued



User information for Pat M and Doug is added into the computer database by using the User Editor.

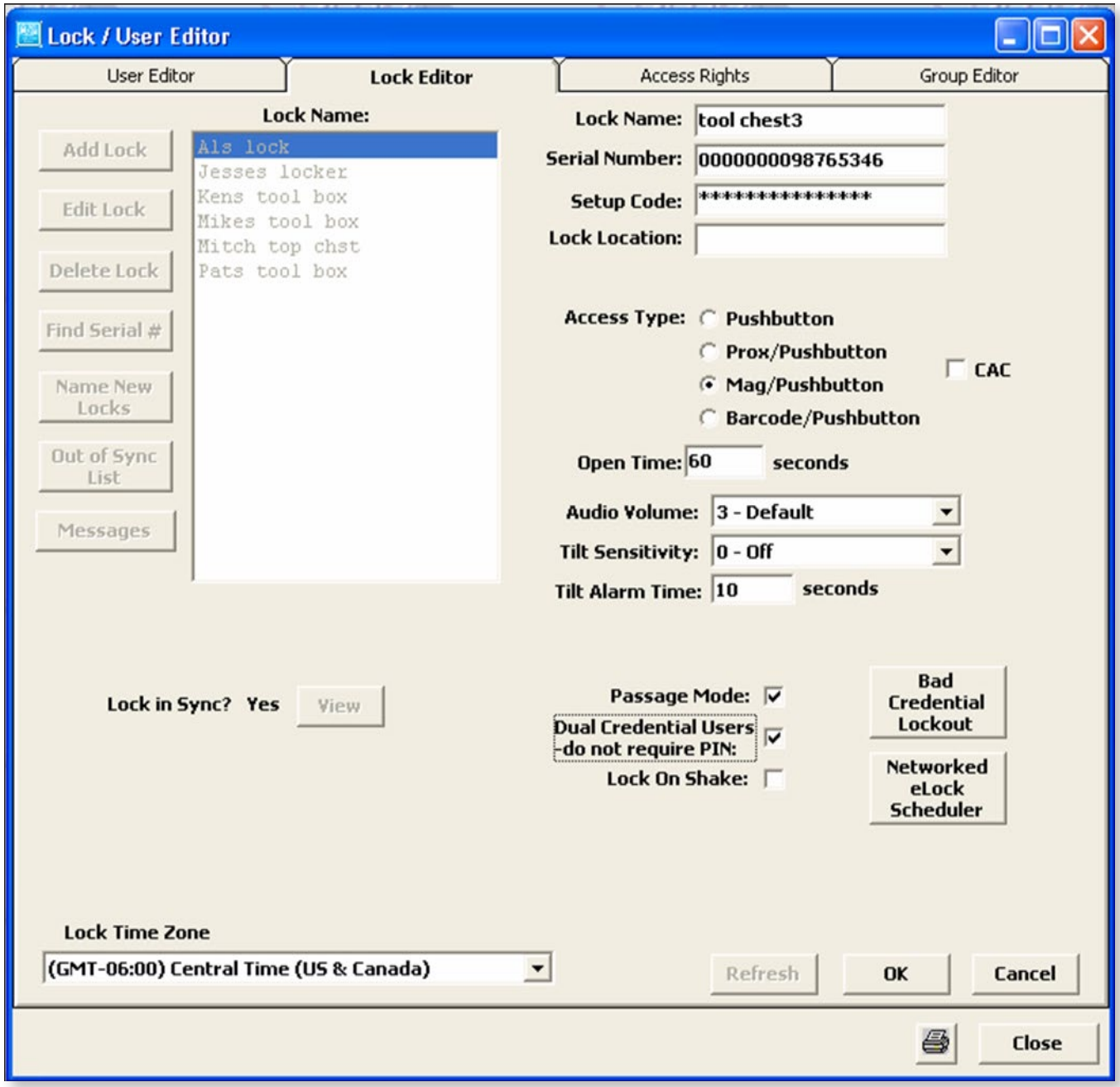
PROGRAMMING EXAMPLE *continued*

The new users do not have any access rights to locks.

3. Open **Lock Editor.**
4. Select **Add Lock**.

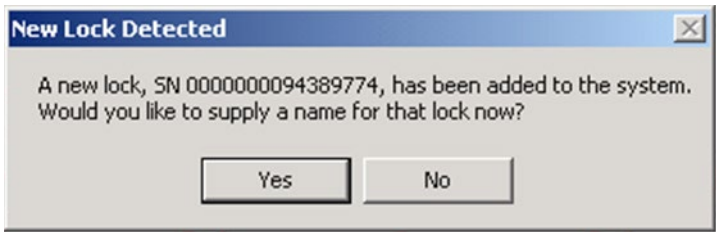
NOTE: *The screen below is of a new lock being added to the computer database.*

5. There are two different ways to enter a lock into the **Lock Editor**; manually or automatically. To enter the information manually, click **Add Lock** and enter the information into the screen. (See pages 15-24 for more information.)

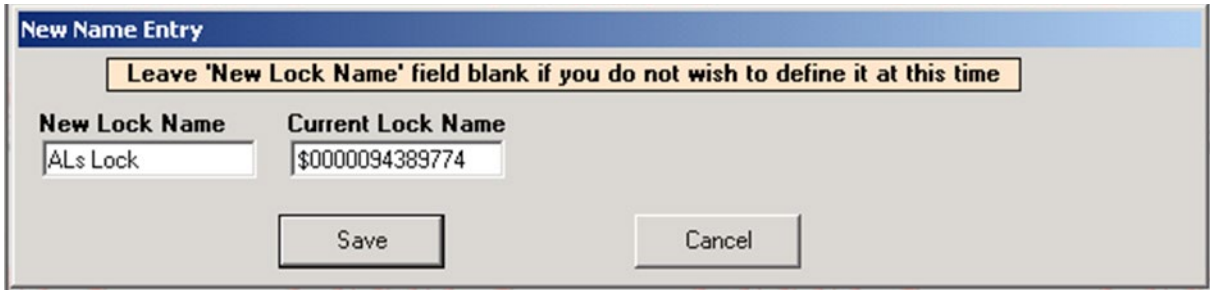


PROGRAMMING EXAMPLE continued

6. Alternately, the lock can automatically be added to the database.
   a. Press and hold "CLEAR" on the access panel. "SETUP CODE" will appear on the display.
   b. Enter the setup code that was provided on the sticker set with the lock into the keypad.
   c. Choose "1-UNLOCK."
   d. "SETUP READY" will appear on the display.
   e. Connect the USB dongle to the computer and route the 6 wire RJ11 cable from the dongle to the lock. If a network module is being used and it is setup, press the "Up" button to initiate a manual update.
   f. Within a few seconds, the following window will appear, SNXXXX is the serial number of the lock being added.


New Lock Detected
A new lock, SN 0000000094389774, has been added to the system.
Would you like to supply a name for that lock now?
Yes
No

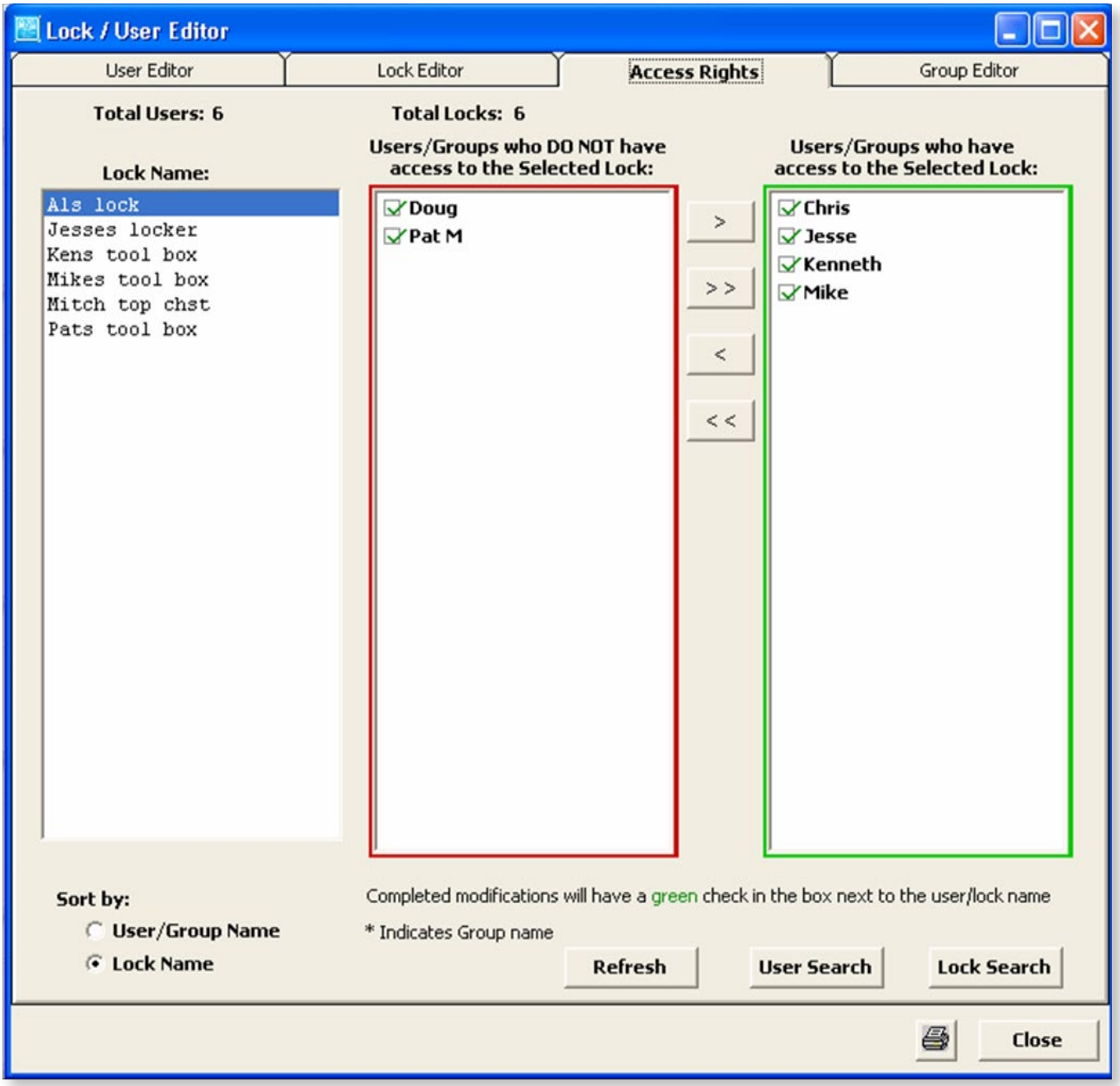
   g. Click **Yes.**
   h. Enter the **New Lock Name**. The lock and all of the settings will be loaded into the database.



   i. Click **Save**.

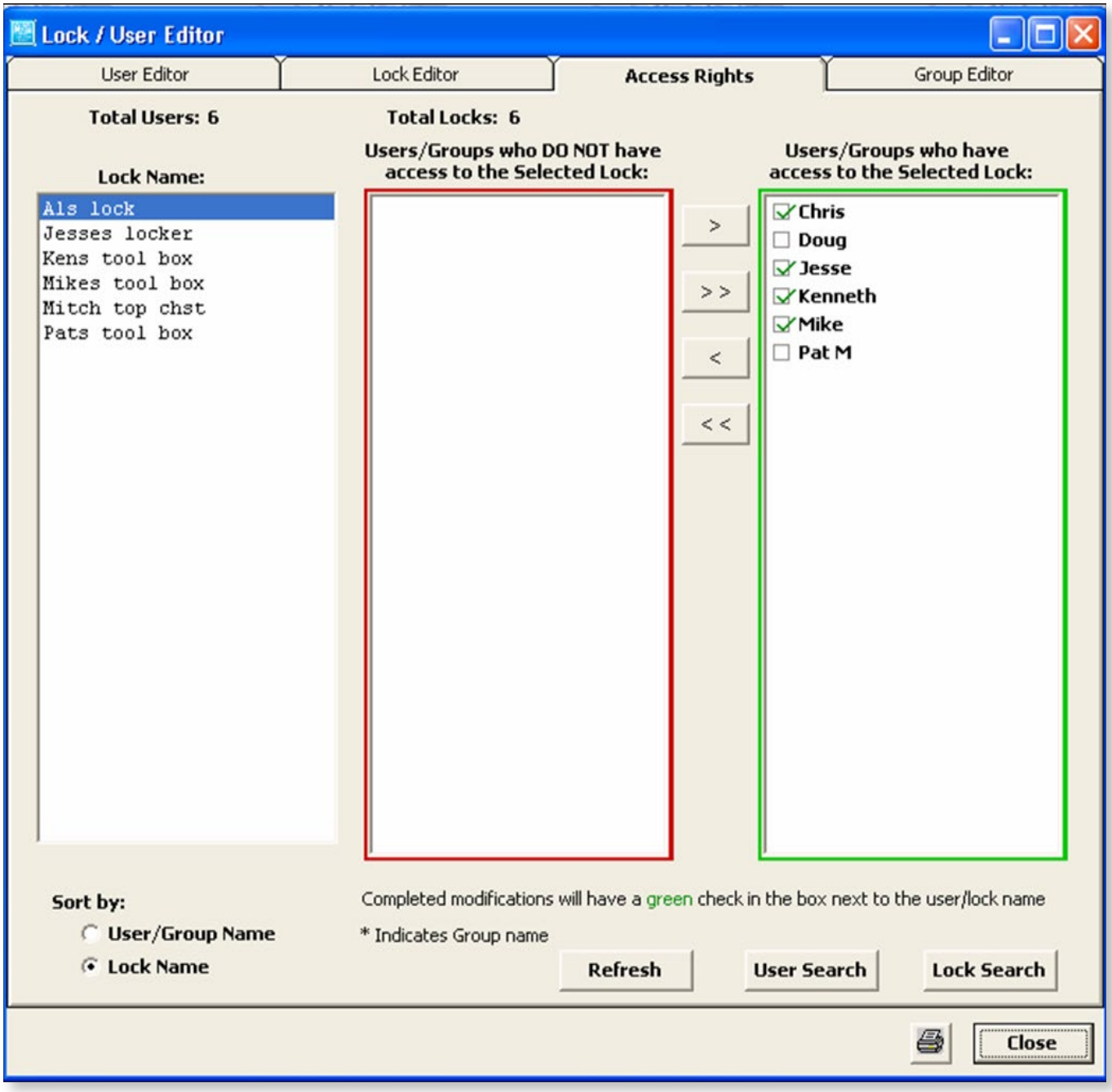
PROGRAMMING EXAMPLE *continued*

Click Access Rights tab. The screen below shows users Doug and Pat M DO NOT have access to the ALs lock.



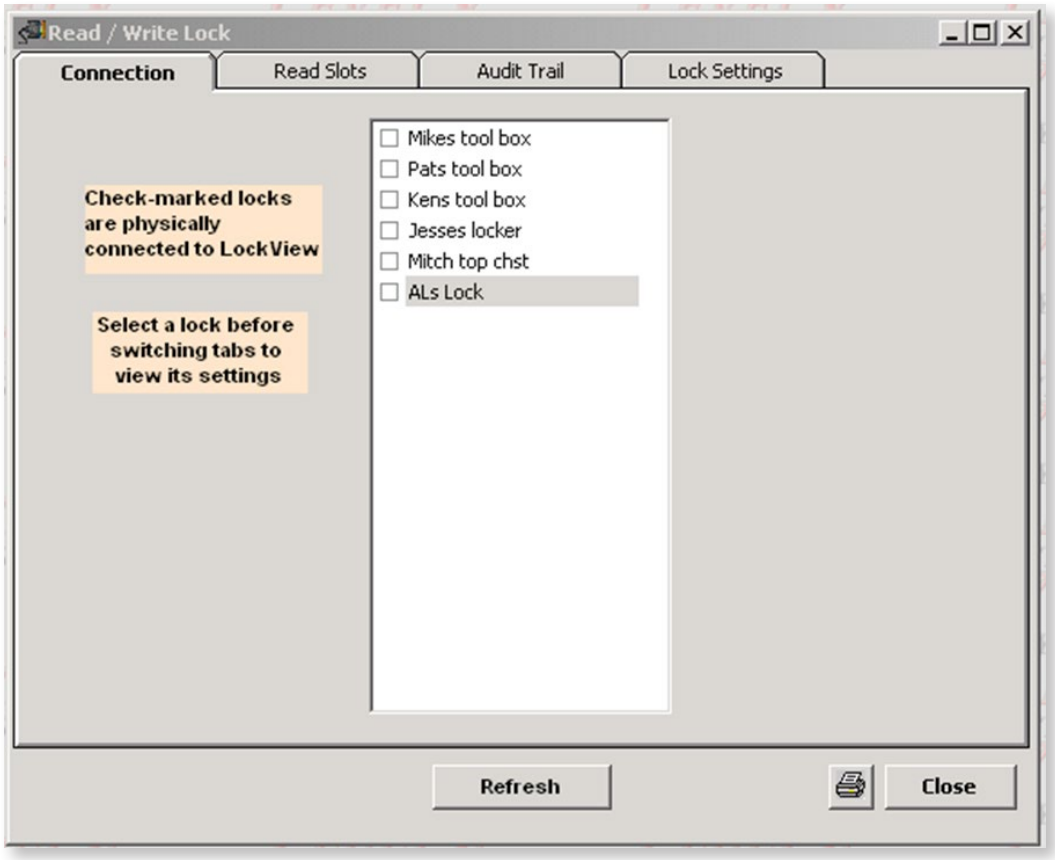
PROGRAMMING EXAMPLE *continued*

By highlighting Doug and Pat M and selecting the appropriate arrow, these two new users are granted access to ALs lock as it shows in the next screen (which is the contents of the computer's database), but they still are not able to open the lock until they are uploaded into the lock's database. The two new users will not have a check mark next to their names and will not be able to open the ALs lock until they are uploaded into the lock's database. When they are uploaded, a check mark will appear in the box next to their names in the right column.



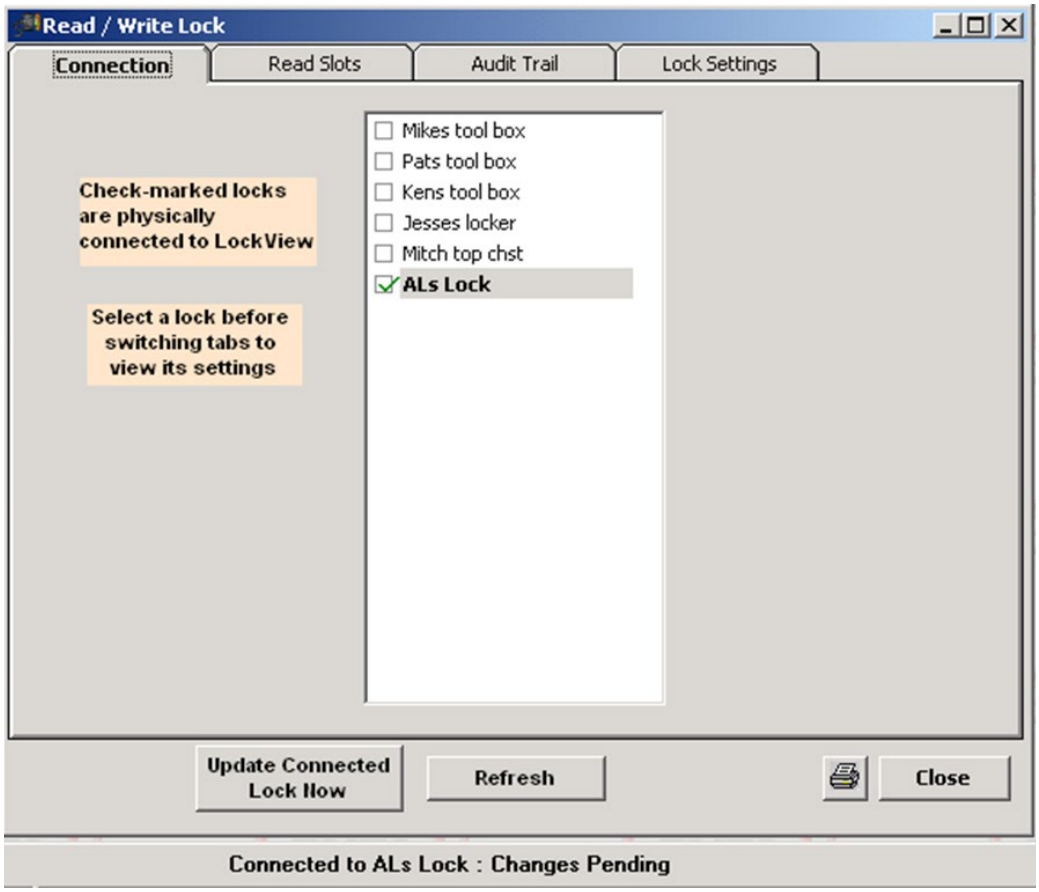
Open the **Read/Write Lock** menu. Choose the **Connection** tab.

PROGRAMMING EXAMPLE *continued*



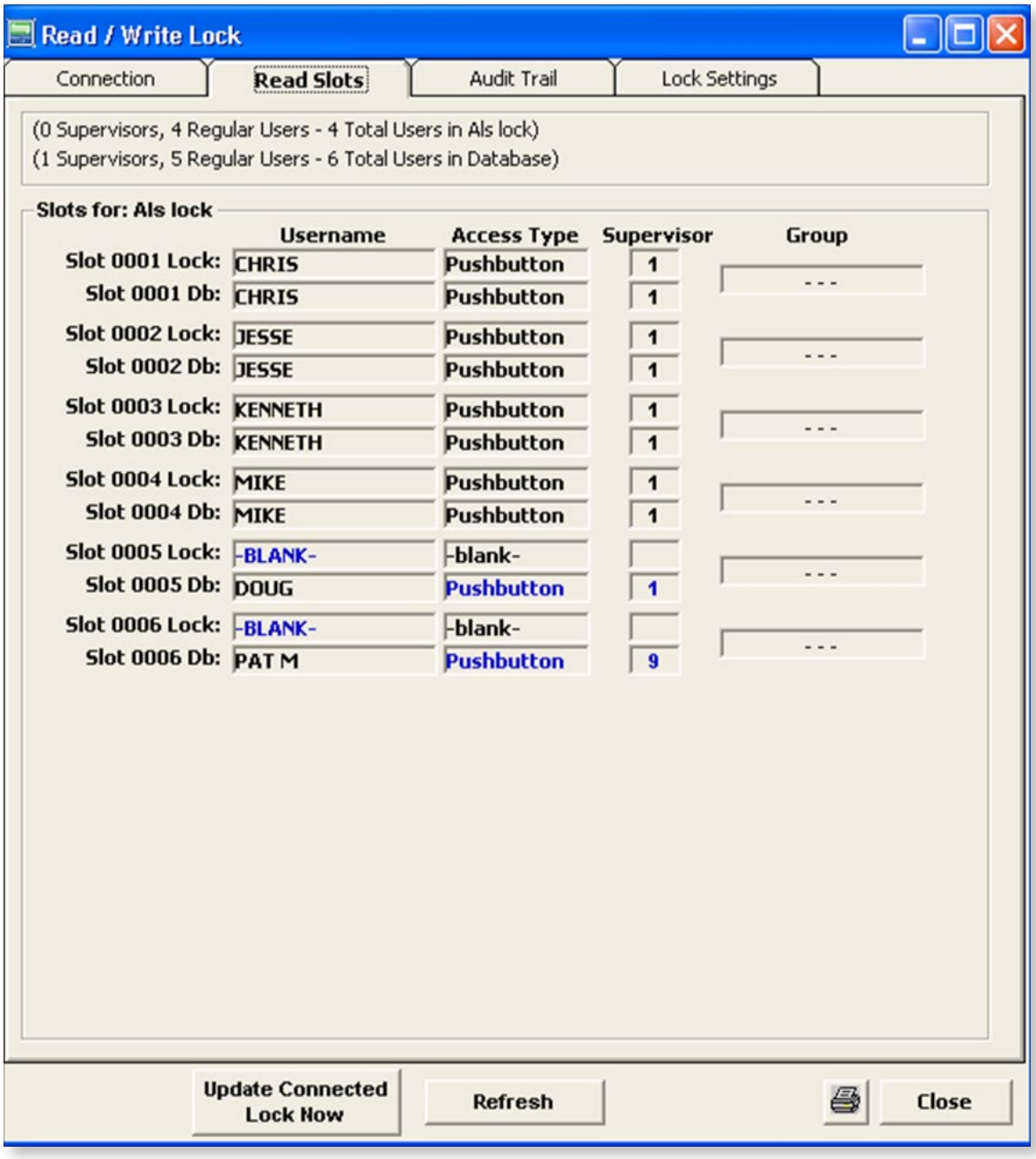
NOTE: *There are no highlighted locks or check marks.*

Plug in the USB dongle into the computer and plug in the RJ11 cable into the lock. "**Connected to ALs Lock**" appears on the status bar as well as a check appears next to ALs lock.



PROGRAMMING EXAMPLE continued

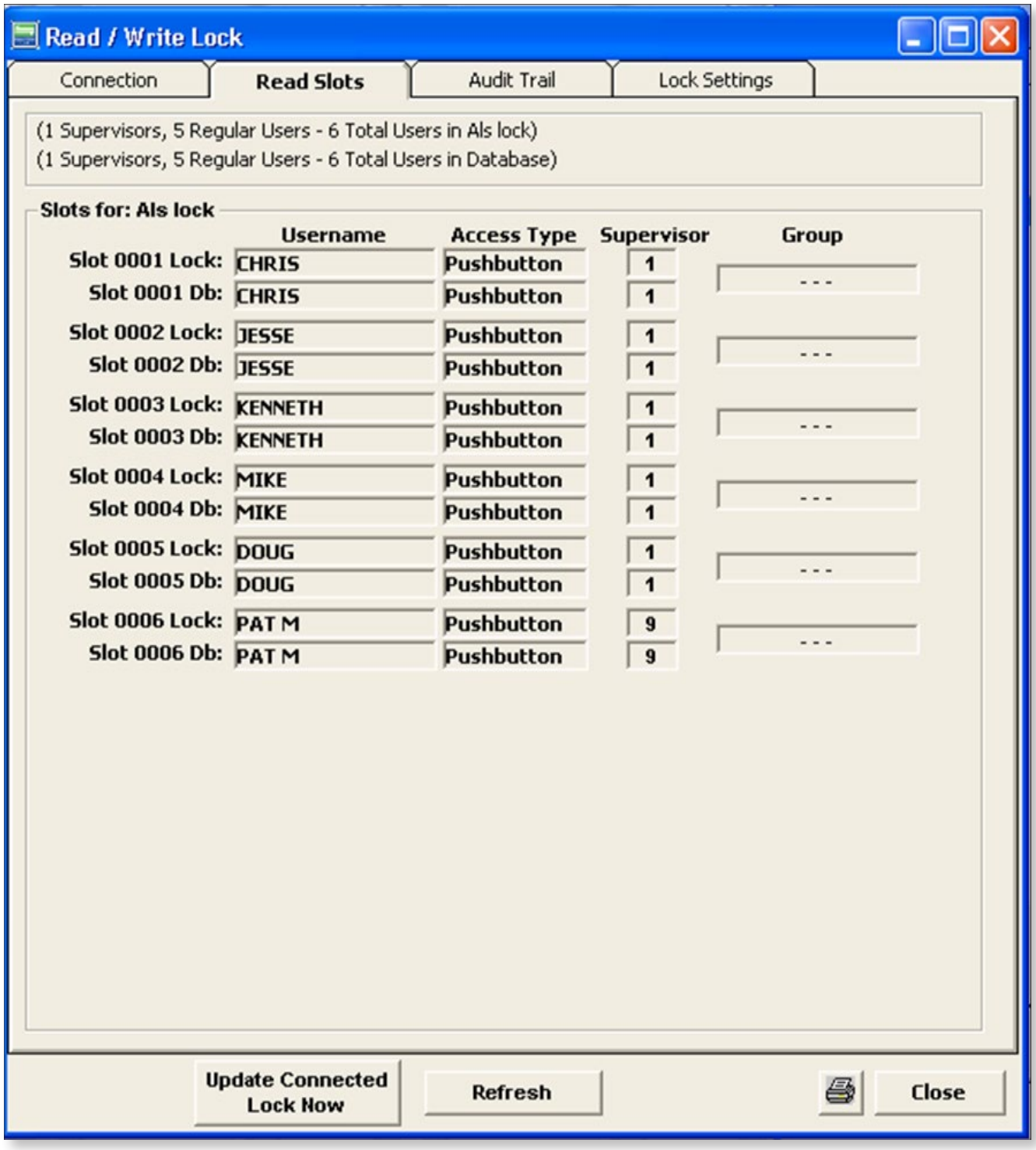
7. Select **Read Slots**.


Read / Write Lock
Connection
Read Slots
Audit Trail
Lock Settings
(0 Supervisors, 4 Regular Users - 4 Total Users in Als lock)
(1 Supervisors, 5 Regular Users - 6 Total Users in Database)
Slots for: Als lock
Username
Access Type
Supervisor
Group
Slot 0001 Lock: CHRIS Pushbutton 1
Slot 0001 Db: CHRIS Pushbutton 1
Slot 0002 Lock: JESSE Pushbutton 1
Slot 0002 Db: JESSE Pushbutton 1
Slot 0003 Lock: KENNETH Pushbutton 1
Slot 0003 Db: KENNETH Pushbutton 1
Slot 0004 Lock: MIKE Pushbutton 1
Slot 0004 Db: MIKE Pushbutton 1
Slot 0005 Lock: -BLANK- -blank-
Slot 0005 Db: DOUG Pushbutton 1
Slot 0006 Lock: -BLANK- -blank-
Slot 0006 Db: PAT M Pushbutton 9
Update Connected Lock Now
Refresh
Close

This **Read Slots** screen shows the new users Doug and Pat M in the computer's database in slots 0005 and 0006, but not in the ALs Lock database. [It is possible that the system already performed the update automatically.]

8. Press **Update Connected Lock Now**.

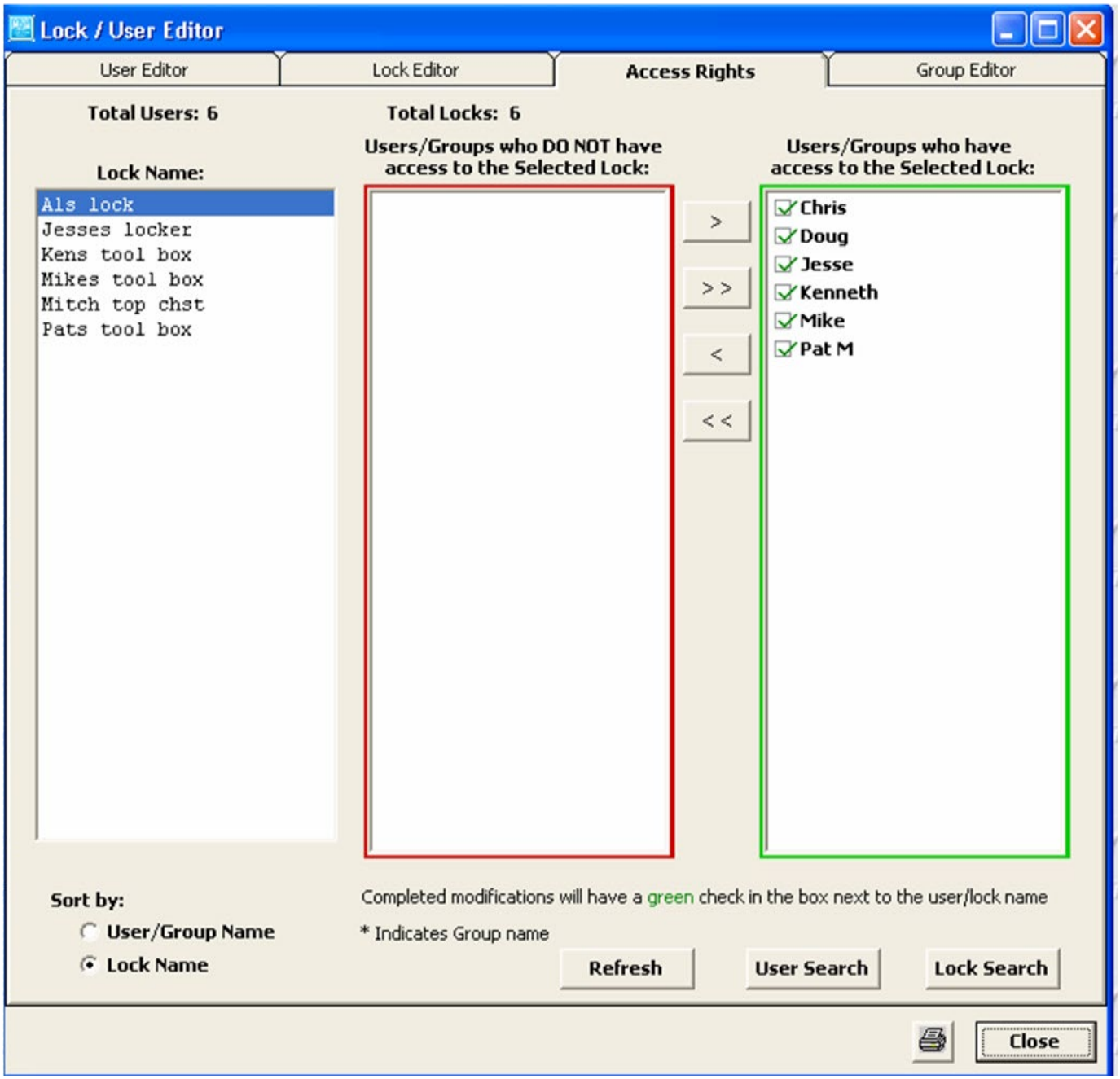
PROGRAMMING EXAMPLE *continued*


Read / Write Lock
Connection
Read Slots
Audit Trail
Lock Settings
(1 Supervisors, 5 Regular Users - 6 Total Users in Als lock)
(1 Supervisors, 5 Regular Users - 6 Total Users in Database)
Slots for: Als lock
Username
Access Type
Supervisor
Group
Slot 0001 Lock: CHRIS Pushbutton 1 - - -
Slot 0001 Db: CHRIS Pushbutton 1
Slot 0002 Lock: JESSE Pushbutton 1 - - -
Slot 0002 Db: JESSE Pushbutton 1
Slot 0003 Lock: KENNETH Pushbutton 1 - - -
Slot 0003 Db: KENNETH Pushbutton 1
Slot 0004 Lock: MIKE Pushbutton 1 - - -
Slot 0004 Db: MIKE Pushbutton 1
Slot 0005 Lock: DOUG Pushbutton 1 - - -
Slot 0005 Db: DOUG Pushbutton 1
Slot 0006 Lock: PAT M Pushbutton 9 - - -
Slot 0006 Db: PAT M Pushbutton 9
Update Connected Lock Now
Refresh
Close

New users Doug and Pat M are now updated in ALs Lock.

PROGRAMMING EXAMPLE *continued*

Open **Lock/User Editor**. Select **Access Rights**.

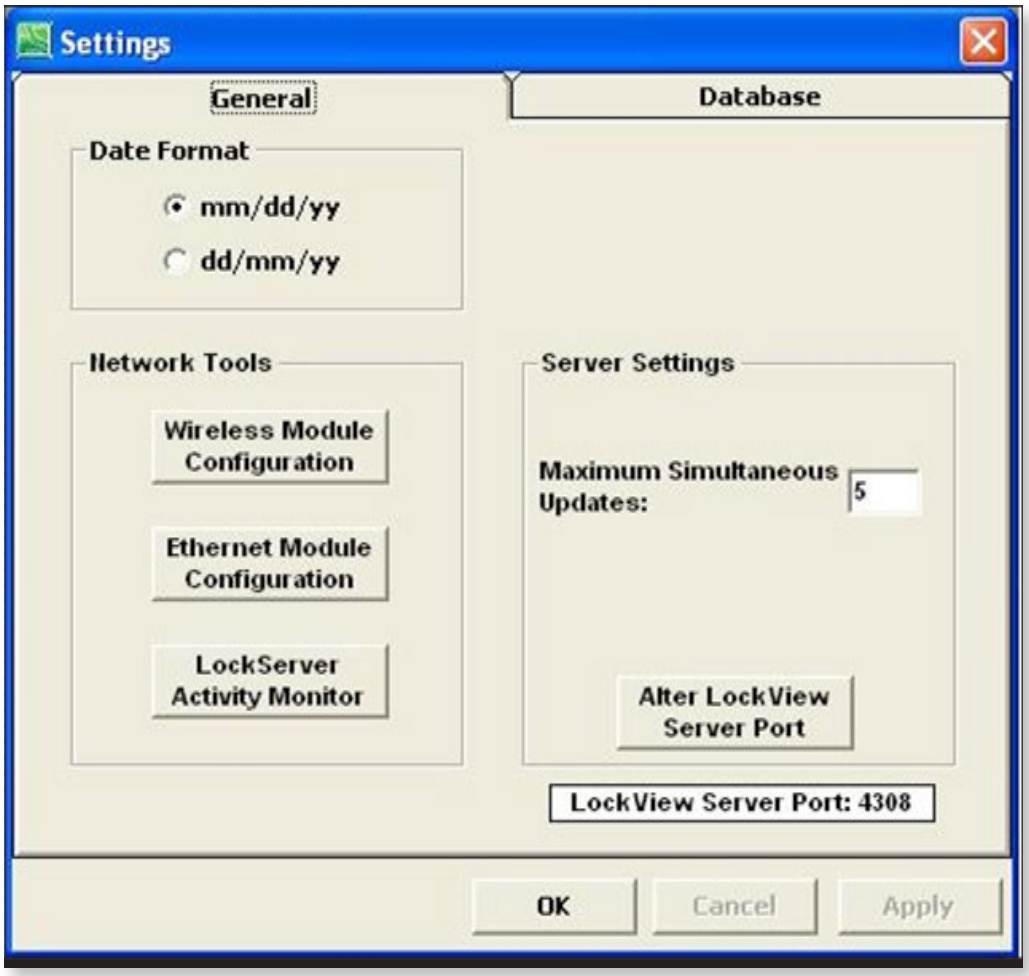


The **Access Rights** screen now shows a check mark next to Doug and Pat M.

SETTINGS

Settings window allows the Operator to make changes to the database location on the computer as well as other changes to LockView.

- Select the **Settings** window.



- **GENERAL** tab
  Date Format (Changes date format in Audit Log)
  month/day/year
  Or
  day/month/year

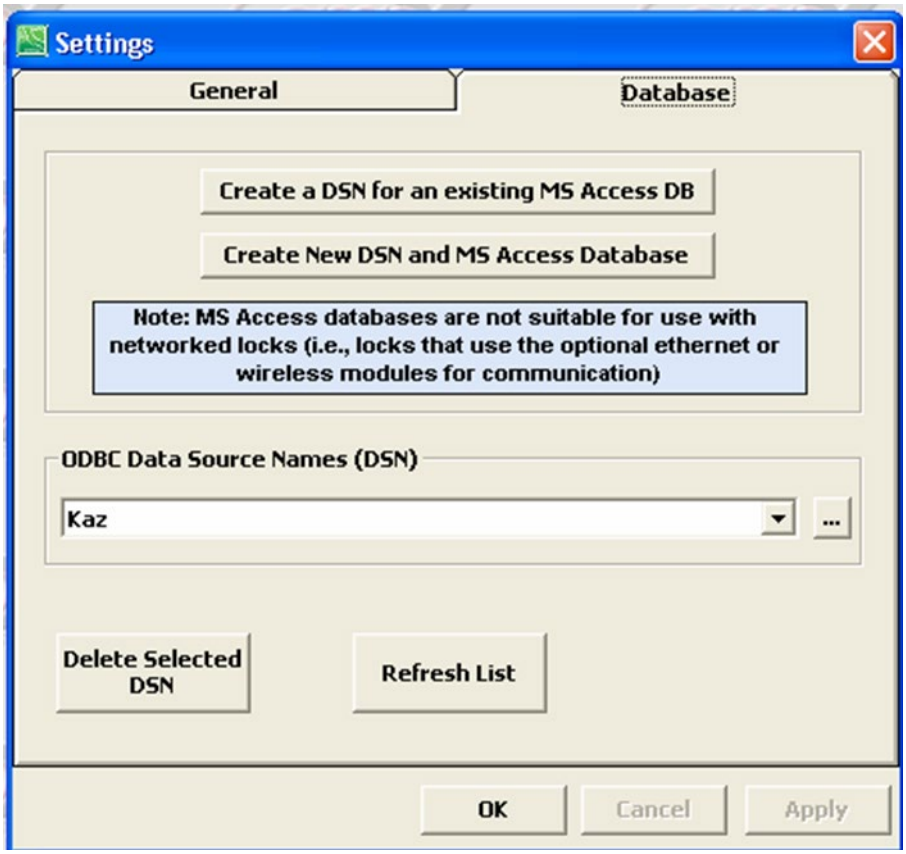
- **NETWORK TOOLS** (Refer to "Database & Network Configuration & Install Manual")

- **SERVER SETTINGS (NETWORKED SYSTEMS ONLY)**
  Maximum Simultaneous Updates: The number of locks the lock server can update simultaneously.
- **Alter LockView Server Port**: TCP/UDP Port 4308 is CompX-LockView owned. No other software should use this port. It is highly recommended NOT to alter the TCP port.

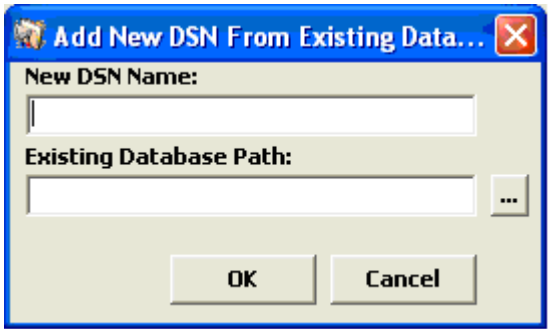
- **DATABASE** tab (Refer to "Database & Network Configuration & Install Manual")

CREATE ODBC CONNECTION FOR AN EXISTING ACCESS DATABASE

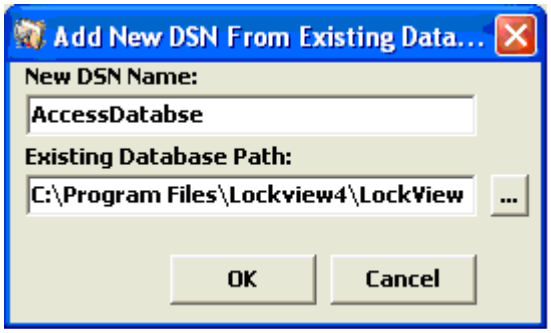
1. Open LockView, open **LockView Options**, select the **Database** tab.


Settings
General
Database
Create a DSN for an existing MS Access DB
Create New DSN and MS Access Database
Note: MS Access databases are not suitable for use with networked locks (i.e., locks that use the optional ethernet or wireless modules for communication)
ODBC Data Source Names (DSN)
Kaz
...
Delete Selected DSN
Refresh List
OK
Cancel
Apply

2. Select '**Create a DSN for an existing MS Access DB**'

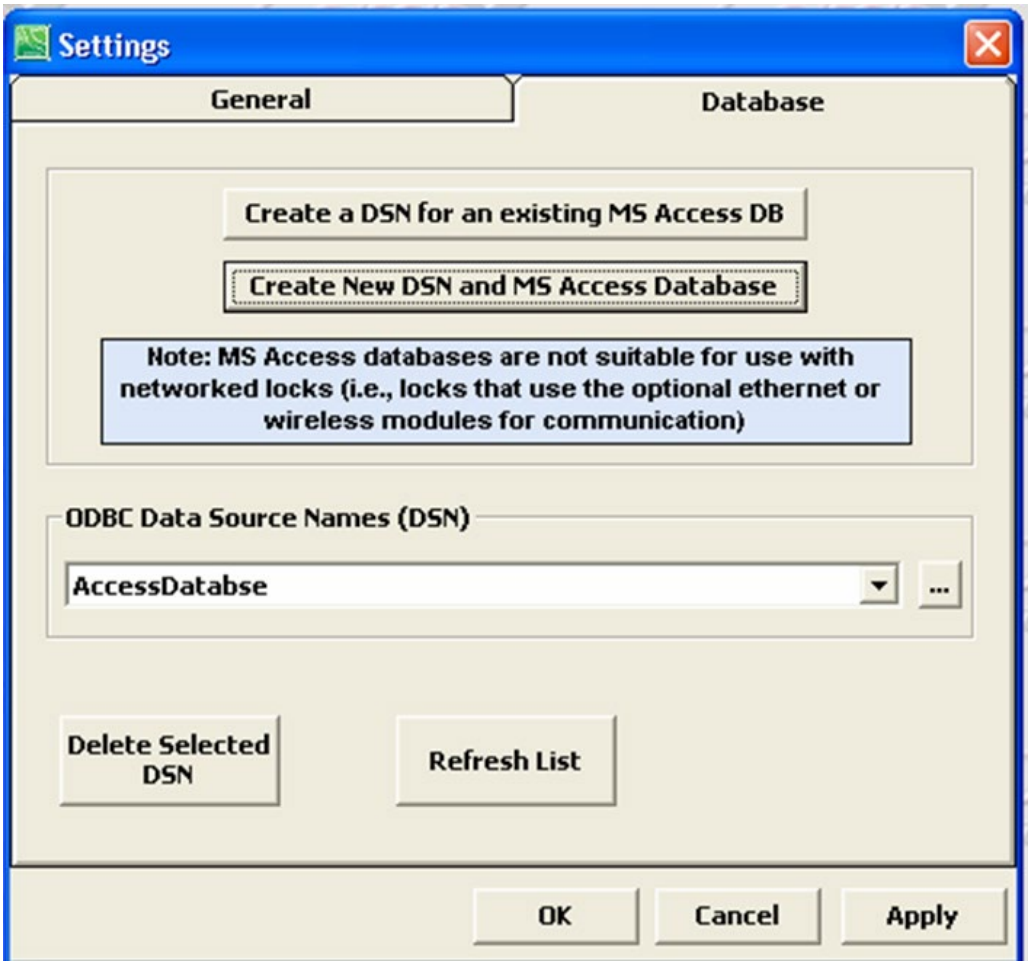


3. Enter a DSN.
   In this case, AccessDatabse was entered for the DSN Name.
   Click on the browse icon (...) and locate the Existing Database,
   Or type in the location and click **OK**.

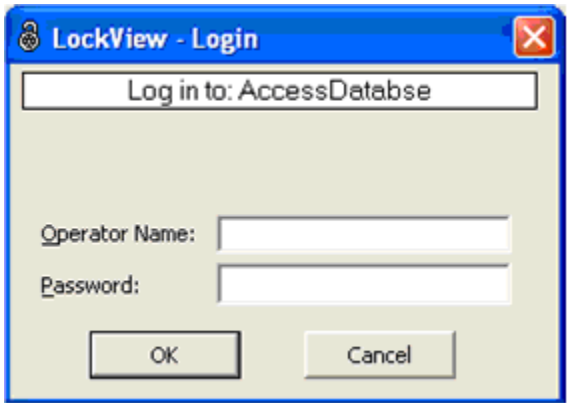


CREATE ODBC CONNECTION FOR AN EXISTING ACCESS DATABASE cont.

4. AccessDatabse is now the current ODBC connection.
   Click '**Apply**.'

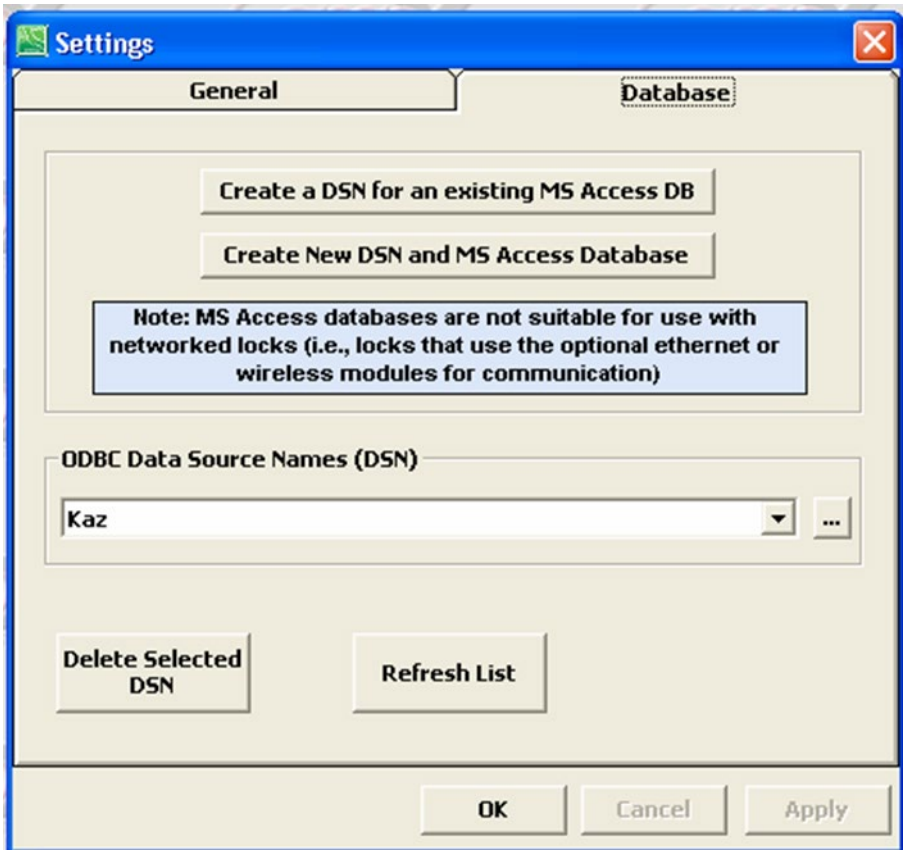

Settings
General
Database
Create a DSN for an existing MS Access DB
Create New DSN and MS Access Database
Note: MS Access databases are not suitable for use with networked locks (i.e., locks that use the optional ethernet or wireless modules for communication)
ODBC Data Source Names (DSN)
AccessDatabse
...
Delete Selected DSN
Refresh List
OK
Cancel
Apply

5. Login to database with an operator that is valid in the chosen database.
   Click **OK**.

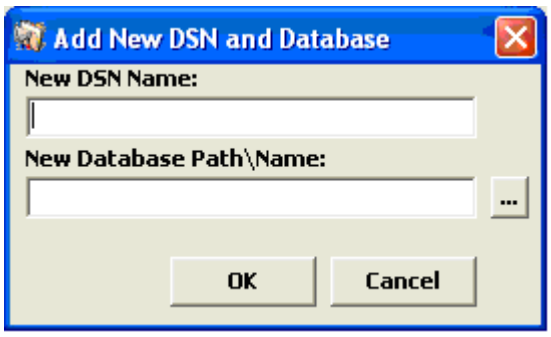


CREATE ODBC CONNECTION FOR A NEW ACCESS DATABASE

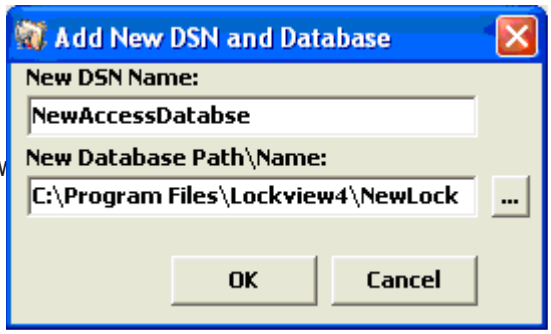
1. Open LockView, select **LockView Options**, click the **Database** tab.


Settings
General
Database
Create a DSN for an existing MS Access DB
Create New DSN and MS Access Database
Note: MS Access databases are not suitable for use with networked locks (i.e., locks that use the optional ethernet or wireless modules for communication)
ODBC Data Source Names (DSN)
Kaz
...
Delete Selected DSN
Refresh List
OK
Cancel
Apply

2. Select '**Create a New DSN and MS Access Database**'

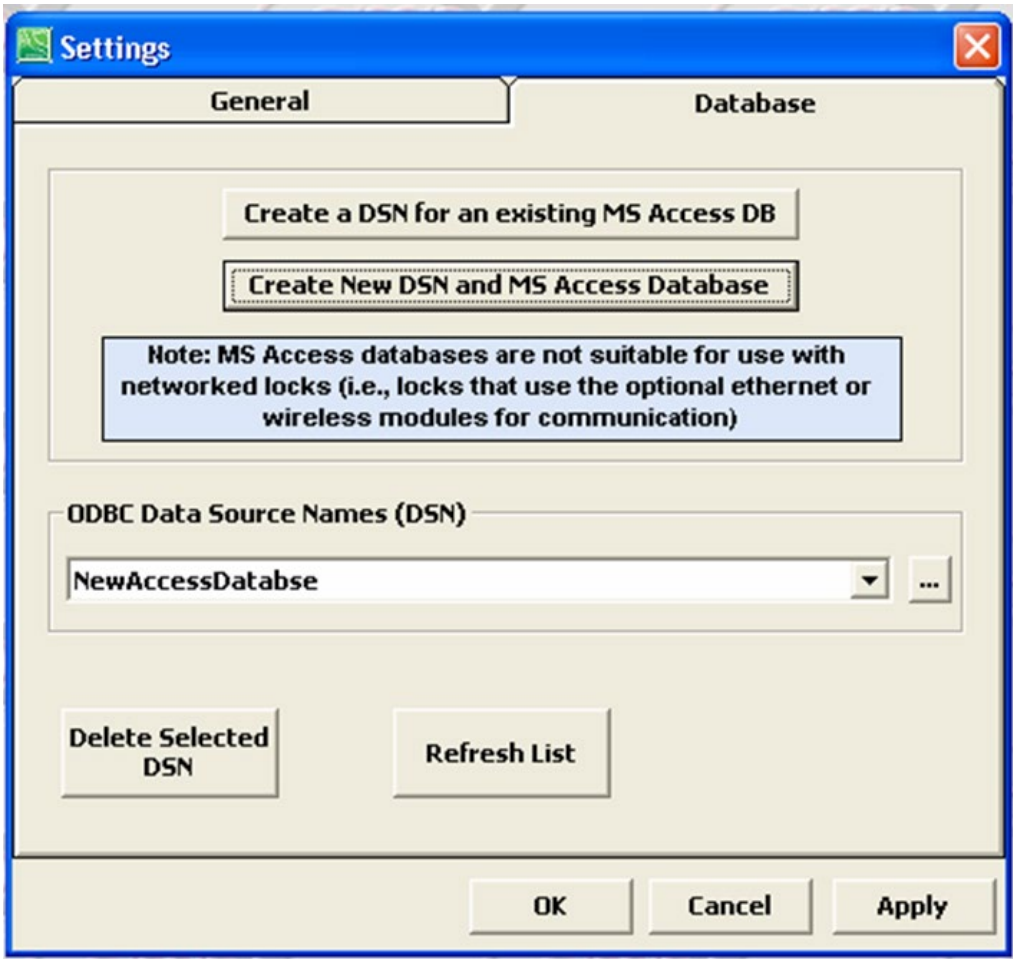


3. Enter a DSN.
   In this case, NewAccessDatabse was entered for the DSN Name.
   Click on the browse icon (...) and select the desired location of the new
   Click **OK**.

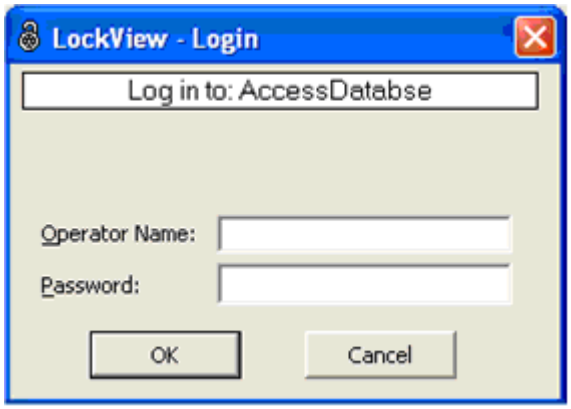


CREATE ODBC CONNECTION FOR A NEW ACCESS DATABASE cont.

4. NewAccessDatabse is now the current ODBC connection.
   Click '**Apply**.'


Settings
General
Database
Create a DSN for an existing MS Access DB
Create New DSN and MS Access Database
Note: MS Access databases are not suitable for use with networked locks (i.e., locks that use the optional ethernet or wireless modules for communication)
ODBC Data Source Names (DSN)
NewAccessDatabse
...
Delete Selected DSN
Refresh List
OK
Cancel
Apply

5. Login to database with:
   Operator Name: *admin*
   Password: *admin*. Click **OK**.



NOTES

LockView® NTC/VTC 4.3.3

LOCKVIEW NTC/VTC INSTRUCTION MANUAL

Instruction Manual

Copyright 2013 © CompX Security Products
Any companies and/or products referred to herein are marks or registered trademarks of their respective companies, owners and/or mark holders.

Snap-on®